PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-222360

(43)Date of publication of application : 11.08.2000

---

(51)Int.Cl. G06F 15/00
G06F 12/14
G06F 13/00
G06K 17/00
H04L 9/32

---

(21)Application number : 11-024446 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 01.02.1999 (72)Inventor : SHIBATA AKIO
TAKAYAMA HISASHI

---

(54) METHOD AND SYSTEM FOR AUTHENTICATION AND AUTHENTICATION PROCESSING PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To exclude any illegal access by identifying any legal access with a small calculation quantity in single sign on type authentication for permitting plural times of access by single user authentication.
SOLUTION: Secrecy information 4 is shared by a client means 1 and an authentication server means 2. The authentication server means 2 issues an authentication ticket 5 including collation information obtained by performing an irreversible arithmetic operation (f) on the secrecy information 4 (n) times. The client

means 1 indicates this authentication ticket and presentation information obtained by performing an irreversible arithmetic operation (f) on the secrecy information 4 (n-k) times to a permission server means 3. The permission server means 3 performs the irreversible arithmetic operation (f) on the presented information (k) times, and checks whether or not this presented information matches the collation information. In this case, (k) is increased from 1 to (n) so that the authentication ticket 5 can be used for the maximum (n) times of access without calculating the next presented information from the past presented information.

CLAIMS

[Claim(s)]
[Claim 1]An authentication server means to publish an authentication ticket.
An approval server means to which use of an authentication ticket is approved, and a client means which requires an authentication ticket of said authentication server means, and requires use approval of an authentication ticket of said approval server means.
A client means which it is the authentication system provided with the above, and the number of times of effective holds an authentication ticket which is n (n is a positive integer), shows this, and asks for use approval, Provide an approval server means to which presentation information is required of said client means in response, it compares with said authentication ticket, and use is approved, and said authentication ticket, Including a ticket identifier, collation information, and the number of times of effective, he is given by attestation child and said collation information, Predetermined irreversible arithmetic operation is performed to confidential information which said authentication server means and said client means share n times, Said presentation information in case a use count of said authentication ticket is k (k is a positive integer below n) performs said predetermined irreversible arithmetic operation to said

confidential information n-k times.

[Claim 2]The authentication system according to claim 1, wherein said authentication server means manages user authentication information, performs a user authentication procedure between said client means and publishes said authentication ticket.

[Claim 3]In a user authentication procedure, generate a random number, and said authentication server means shows this, requires attestation presentation information of said client means, and it said confidential information, The authentication system according to claim 2, wherein it performs said predetermined irreversible arithmetic operation to connection by said user authentication information and said random numbers once or more and said attestation presentation information performs said predetermined irreversible arithmetic operation to said confidential information n times.

[Claim 4]Said authentication server means generates a random number in a user authentication procedure, shows this, and requires attestation presentation information of a client means, Said attestation presentation information is an EXCLUSIVE-OR-operation result of what performed said predetermined irreversible arithmetic operation to connection by said user authentication information and said random numbers once or more, and a random number for attestation which said client means generated, The authentication system according to claim 2, wherein said confidential information is said random number for attestation counted backward from said attestation presentation information.

[Claim 5]The authentication system according to any one of claims 2 to 4, wherein said user authentication information is a password entered by user.

[Claim 6]The authentication system according to any one of claims 2 to 4, wherein said user authentication information is the common key system encryption key held in secrecy.

[Claim 7]The authentication system according to any one of claims 1 to 6, wherein said attestation child is a message authorization code.

[Claim 8]The authentication system according to any one of claims 1 to 6, wherein said attestation child is a digital signature.

[Claim 9]The authentication system according to any one of claims 1 to 8, wherein said predetermined irreversible arithmetic operation is tropism hash operation on the other hand.

[Claim 10]The authentication system according to any one of claims 1 to 9, wherein said authentication ticket contains a server identifier.

[Claim 11]The authentication system according to any one of claims 1 to 10, wherein said authentication ticket includes the time of the date of issue.

[Claim 12]Said authentication ticket including a publisher identifier said approval

server means, While carrying out use approval, collation information of said authentication ticket, the number of times of effective, the time of the date of issue, a publisher identifier, and an attestation child are updated, The authentication system according to claim 11, wherein said collation information is updated by what performed said predetermined irreversible arithmetic operation to said confidential information n-k times and said number of times of effective is updated by n-k.

[Claim 13]The authentication system according to any one of claims 1 to 12, wherein said approval server means has managed a use count of said authentication ticket, shows this and requires presentation information.

[Claim 14]The authentication system according to any one of claims 1 to 12, wherein said client means has managed a use count of said authentication ticket, shows this with said authentication ticket and asks for use approval.

[Claim 15]Have said two or more approval server means and an authentication ticket management tool which manages a use count of said authentication ticket, and said client means, Have managed a use count of said authentication ticket, with said authentication ticket, this is shown, ask for use approval, and said authentication server means, While publishing said authentication ticket, point to shelf registration of said authentication ticket to said authentication ticket management tool, and said approval server means, The authentication system according to any one of claims 1 to 11 not carrying out use approval when it points to renewal of a history of said authentication ticket to said authentication ticket management tool in response to presentation of said authentication ticket and a rejected note is received from said authentication ticket management tool.

[Claim 16]Said approval server means two or more preparations and said client means, Have managed a use count of said authentication ticket, with said authentication ticket, this is shown, ask for use approval, and said authentication server means, Memorize an issuance history, while publishing said authentication ticket, and said approval server means, Memorize an update history, while updating said authentication ticket, and it refers for a history of said authentication ticket to said authentication server means which a publisher identifier of said authentication ticket shows in response to presentation of said authentication ticket, or said approval server means, The authentication system according to claim 12 not carrying out use approval when a rejected note is received from said authentication server means or said approval server means.

[Claim 17]It is what said approval server means generates a random number in a use approval procedure, shows this, and requires presentation information, The authentication system according to any one of claims 14 to 16, wherein said presentation information in case a use count of said authentication ticket is k is an EXCLUSIVE-OR-operation result of what performed said predetermined irreversible arithmetic operation to said confidential information n-k times, and said random

number.

[Claim 18]An authentication server means to publish an authentication ticket.

An approval server means to which use of an authentication ticket is approved, and a client means which requires an authentication ticket of said authentication server means, and requires use approval of an authentication ticket of said approval server means.

An input means from which it is the authentication system provided with the above, and said client means obtains an input of the number of times of effective of a user-identification child, user authentication information, a server identifier, and an authentication ticket, Ticket holding mechanism which obtains and holds an authentication ticket from said authentication server means, and is shown to said approval server means, A processing selecting means which acquires existence information on an authentication ticket and chooses processing from said ticket holding mechanism, A hash means to obtain a random number and to perform hash operation to these connection from said authentication server means while acquiring user authentication information from said input means, A secret memory measure which memorizes in secrecy a hash value obtained from said hash means, Take out a hash value from said secret memory measure, and the number of times n of effective (n is a positive integer) is obtained from said input means in a user authentication procedure, A multi stage hash value which performed and obtained hash operation of n stage is sent to said authentication server means, In a use approval procedure, the using frequency k (k is a positive integer below n) is obtained from said approval server means, An authentication information storage means which possessed a multi stage hash means to send a multi stage hash value which performed and obtained hash operation of a n-k stage to said approval server means and in which user authentication information was accumulated for said authentication server means, The 2nd multi stage hash means that performs n+1 step of hash operation to connection by random number generating means which generates a random number and is sent to said client means, and user authentication information acquired from said authentication information storage means and a random number generated by said random number generating means, An attestation collation means compared with a multi stage hash value which obtained a multi stage hash value obtained from said client means by said 2nd multi stage hash means, a ticket identifier creating means which generates an effective ticket identifier, and attestation which clocks time and outputs time information -- a time check -- with a means. A ticket identifier obtained from said ticket identifier creating means, a multi stage hash value obtained from said attestation collation means, a server identifier obtained from said client means and the number of times of effective, and said attestation -- a time check -- a time stamp based on time information acquired from a means. And an attestation child is added to connection of a publisher identifier which shows an authentication server means,

approval which an attestation child addition means sent to said client means as an authentication ticket is provided, and said approval server means clocks an attestation child verifying means which verifies an attestation child of an authentication ticket who got from said client means, and time, and outputs time information -- a time check -- with a means. the validity of a server identifier and a time stamp, and said approval -- a time check -- with a ticket effective judging means which checks the validity of a difference with time information acquired from a means. A ticket use management tool which remains with a ticket identifier of an authentication ticket, and using frequency, and manages the number of times of available, The 3rd multi stage hash means that outputs a secondary multi stage hash value which performed and obtained hash operation of k stage from said ticket use management tool to a multi stage hash value which obtained the using frequency k and was obtained from said client means, An approval collation means which compares a multi stage hash value obtained from said ticket use management tool and a secondary multi stage hash value obtained from said 3rd multi stage hash means is provided.

[Claim 19]The authentication system comprising according to claim 18:
A server common key memory measure said attestation child addition means remembers a common key system encryption key shared between servers to be.
A self-identifier storage means which memorizes a self-identifier.
Data connecting mechanism which connects a ticket identifier, a multi stage hash value, the number of times of effective, a time stamp, a server identifier, and a publisher identifier obtained from said self-identifier storage means.
A connection data hash means to perform hash operation to connection data obtained from said data connecting mechanism, A common key system cryptographer stage which enciphers a hash value obtained from said connection data hash means using a common key system encryption key obtained from said server common key memory measure, and is made into an attestation child, Attestation child connecting mechanism which connects connection data obtained from said data connecting mechanism and an attestation child who got from said common key system cryptographer stage is provided, The 2nd server common key memory measure that memorizes a common key system encryption key which said attestation child verifying means shares between servers, Attestation child separating mechanism which divides an authentication ticket into connection data and an attestation child, A data separation means which divides into a ticket identifier, a multi stage hash value, the number of times of effective, a time stamp, a server identifier, and a publisher identifier connection data obtained from said attestation child separating mechanism, The 2nd connection data hash means that performs hash operation to connection data obtained from said attestation child separating mechanism, The 2nd common key

system cryptographer stage that enciphers a hash value obtained from said 2nd connection data hash means using a common key system encryption key obtained from said 2nd server common key memory measure, and is made into an attestation child for comparison, A publisher identifier collation means which confirms that a publisher identifier obtained from said data separation means is an effective server identifier, A comparison means to compare an attestation child for comparison who got from said 2nd common key system cryptographer stage with an attestation child who got from said attestation child separating mechanism when a collated result obtained from said publisher identifier collation means showed validity, and to output a result.

[Claim 20]The authentication system comprising according to claim 18:
A self-secret key memory measure said attestation child addition means remembers a public key system code secret key of an authentication server to be in secrecy.
A self-identifier storage means which memorizes a self-identifier.
Data connecting mechanism which connects a ticket identifier, a multi stage hash value, the number of times of effective, a time stamp, a server identifier, and a publisher identifier obtained from said self-identifier storage means.
A connection data hash means to perform hash operation to connection data obtained from said data connecting mechanism, A public key system cryptographer stage which enciphers a hash value obtained from said connection data hash means using a public key system code secret key obtained from said self-secret key memory measure, and is made into an attestation child, Attestation child separating mechanism which possesses attestation child connecting mechanism which connects connection data obtained from said data connecting mechanism, and an attestation child who got from said public key system cryptographer stage and from which said attestation child verifying means separates an authentication ticket into connection data and an attestation child, A data separation means which separates into a ticket identifier, a multi stage hash value, the number of times of effective, a time stamp, a server identifier, and a publisher identifier, and outputs connection data obtained from said attestation child separating mechanism, The 2nd connection data hash means that performs hash operation to connection data obtained from said attestation child separating mechanism, A server public key accumulation means which outputs a public key system code public key corresponding to a publisher identifier which a public key system code public key of an effective server was accumulated, and was obtained from said data separation means, A public key system decoding means which decodes an attestation child who got from said attestation child separating mechanism using a public key system code public key obtained from said server public key accumulation means, and is made into a hash value for comparison, A comparison means to compare a hash value obtained from said connection data hash means with a

hash value for comparison obtained from said public key system decoding means, and to output a result.

[Claim 21]Said client means possesses an authentication random number creating means and the 1st exclusive OR means, and them said random number generating means for attestation, In a user authentication procedure, generate a random number for attestation, and said 1st exclusive OR means, A disturbance hash value which obtained by performing EXCLUSIVE OR operation of a random number for attestation obtained from said random number generating means for attestation in a user authentication procedure and a hash value obtained from said hash means is sent to said authentication server means, Memorize said secret memory measure in secrecy, and a random number for attestation obtained from said random number generating means for attestation said multi stage hash means, Take out a random number for attestation from said secret memory measure, and the using frequency k is obtained from said approval server means in a use approval procedure, A multi stage hash value which performed and obtained hash operation of a n−k stage is sent to said approval server means, Said authentication server means possesses the 2nd hash means and 2nd exclusive OR means instead of said attestation collation means, and them said 2nd hash means, Perform hash operation to connection by user authentication information acquired from said authentication information storage means, and random numbers generated by said random number generating means, and said 2nd exclusive OR means, Perform EXCLUSIVE OR operation of a hash value obtained from said 2nd hash means, and a disturbance hash value obtained from said client means, and a random number for attestation is acquired, Perform said 2nd multi stage hash means by random numbers for attestation obtained from said 2nd exclusive OR means, and hash operation of n stage said attestation child addition means, A ticket identifier obtained from said ticket identifier creating means, a multi stage hash value obtained from said 2nd multi stage hash means, a server identifier obtained from said client means and the number of times of effective, and said attestation −− a time check −− a time stamp based on time information acquired from a means. And the authentication system according to any one of claims 18 to 20 adding an attestation child to connection of a publisher identifier which shows an authentication server means, and sending to said client means as an authentication ticket.

[Claim 22]Said approval server means possesses the 3rd hash means and the 2nd attestation child addition means instead of said 3rd multi stage hash means, and them said 3rd hash means, Output a secondary multi stage hash value which performed and obtained hash operation to a multi stage hash value obtained from said client means, and said approval collation means, Compare a multi stage hash value obtained from said ticket use management tool, and a secondary multi stage hash value obtained from said 3rd hash means, and said 2nd attestation child addition means, A ticket

identifier, a server identifier, and the remaining using frequency which were obtained from said ticket use management tool, a multi stage hash value obtained from said client means, and said approval -- a time check -- a time stamp based on time information acquired from a means. And the authentication system according to any one of claims 18 to 21 adding an attestation child to connection of a publisher identifier which shows an approval server means, and sending to said client means as an authentication ticket.

[Claim 23]Have the following and said ticket update indication means, Generate authentication ticket history update indication from a ticket identifier and a server identifier which were obtained from said attestation child verifying means when a decision result obtained from said ticket effective judging means showed validity, and using frequency obtained from said client means, and it sends to said authentication ticket management tool, The using frequency k obtained from said client means when an authentication ticket rejected note was not returned from said authentication ticket management tool, and a multi stage hash value obtained from said attestation child verifying means are outputted, Generate a random number, send said 2nd random number generating means to said client means and said 2nd exclusive OR means, and said 2nd exclusive OR means, Perform EXCLUSIVE OR operation of a random number obtained from said 2nd random number generating means, and a disturbance multi stage hash value obtained from said client means, and a multi stage hash value is acquired, Said 3rd multi stage hash means outputs a secondary multi stage hash value which performed and obtained hash operation of k stage to a multi stage hash value obtained from said 2nd exclusive OR means, Said authentication ticket management tool remains with a ticket identifier and the number of times of effective based on authentication ticket shelf registration directions obtained from said authentication server means, and a group with using frequency is managed, The authentication system according to any one of claims 18 to 21 which checks compatibility with authentication ticket history update indication obtained from said approval server means, and is characterized by sending an authentication ticket rejected note to said approval server means in the case of mismatching.

One or more approval server means.

An authentication ticket management tool which manages issue of an authentication ticket and a using state is provided, Said authentication ticket management tool remains with a ticket identifier and the number of times of effective based on authentication ticket shelf registration directions obtained from said authentication server means, and a group with using frequency is managed, Compatibility with authentication ticket history update indication obtained from said approval server means is checked, In the case of mismatching, send an authentication ticket rejected note at said approval server means, and said authentication server means possesses a ticket registration instruction means, and it said ticket registration instruction

means, A ticket maintenance management tool which generates authentication ticket shelf registration directions from a ticket identifier obtained from said ticket identifier creating means, a server identifier obtained from said client means, and the number of times of effective, and is sent to said authentication ticket management tool, and said client means replaces with said ticket holding mechanism.
Provide the 1st exclusive OR means and said ticket maintenance management tool, Manage using frequency, while obtaining and holding an authentication ticket from said authentication server means, show them to said approval server means, and said multi stage hash means, Take out a hash value from said secret memory measure, and a multi stage hash value which performed and obtained hash operation of n stage in a user authentication procedure is sent to said authentication server means, The using frequency k obtained from said ticket maintenance management tool in a use approval procedure is obtained, Send a multi stage hash value which performed and obtained hash operation of a n-k stage to said 1st exclusive OR means, and said 1st exclusive OR means, A ticket update indication means which performs EXCLUSIVE OR operation of a multi stage hash value obtained from said multi stage hash means, and a random number obtained from said approval server means, and sends a disturbance multi stage hash value of a result to said approval server means, and said approval server means replaces with a ticket use management tool.
The 2nd random number generating means and the 2nd exclusive OR means.

[Claim 24]Have the following and said renewal management tool of a ticket generates ticket use reference from a ticket identifier and a server identifier which were obtained from said attestation child verifying means when a decision result obtained from said ticket effective judging means showed validity, and using frequency obtained from said client means, It sends to said authentication server means or the 2nd approval server means which a publisher identifier shows, When an authentication ticket rejected note is not returned from said authentication server means or said 2nd approval server means, while outputting using frequency obtained from said client means, and a multi stage hash value obtained from said attestation child verifying means, When a ticket identifier, a server identifier, and the remaining using frequency are managed and ticket use reference is received from said 2nd approval server means, the compatibility of using frequency is checked, In the case of mismatching, send an authentication ticket rejected note to said 2nd approval server means, and said 2nd random number generating means, Generate a random number, send to said client means and said 2nd exclusive OR means, and said 2nd exclusive OR means, Perform EXCLUSIVE OR operation of a random number obtained from said 2nd random number generating means, and a disturbance multi stage hash value obtained from said client means, acquire a multi stage hash value, and said 2nd hash means. Output a secondary multi stage hash value which performed and obtained hash

operation to a multi stage hash value obtained from said 2nd exclusive OR means, and said 2nd attestation child addition means, A ticket identifier, a server identifier, and the remaining using frequency which were obtained from said ticket management means, a multi stage hash value obtained from said 2nd exclusive OR means, and said approval -- a time check -- a time stamp based on time information acquired from a means. And the authentication system according to claim 22 which adds an attestation child to connection of a publisher identifier which shows an approval server means, and is characterized by sending to said client means as an authentication ticket.

Provide one or more approval server means, and said authentication server means possesses a ticket issue management tool, and it said ticket issue management tool, A ticket identifier obtained from said ticket identifier creating means, a server identifier obtained from said client means, and the number of times of effective are managed, A ticket maintenance management tool which searches a ticket identifier based on ticket use reference obtained from said approval server means, checks the compatibility of using frequency, and sends an authentication ticket rejected note at said approval server means in the case of mismatching, and said client means replaces with said ticket holding mechanism.

Provide the 1st exclusive OR means and said ticket maintenance management tool, Manage using frequency, while obtaining and holding an authentication ticket from said authentication server means, show them to said approval server means, and said multi stage hash means, Take out a hash value from said secret memory measure, and a multi stage hash value which performed and obtained hash operation of n stage in a user authentication procedure is sent to said authentication server means, The using frequency k obtained from said ticket maintenance management tool in a use approval procedure is obtained, Send a multi stage hash value which performed and obtained hash operation of a n-k stage to said 1st exclusive OR means, and said 1st exclusive OR means, A renewal management tool of a ticket which performs EXCLUSIVE OR operation of a multi stage hash value obtained from said multi stage hash means, and a random number obtained from said approval server means, and sends a disturbance multi stage hash value of a result to said approval server means, and said approval server means replaces with said ticket use management tool.

The 2nd random number generating means and 2nd exclusive OR means.

[Claim 25]An authentication server means to publish an authentication ticket.

An approval server means to which use of an authentication ticket is approved.

A client means which requires an authentication ticket of said authentication server means, and requires use approval of an authentication ticket of said approval server means.

Are the above the authentication method which it had and from an authentication

server means to a client means. . Include predetermined irreversible arithmetic operation for n (n is positive integer) time almsgiving ********** in confidential information which an authentication server means and a client means share. The number of times of effective publishes an authentication ticket which is n, and it a client means, Said authentication ticket is shown in an approval server means, ask for use approval, and to a demand of presentation information on an approval server means a client means, When a use count of said authentication ticket is k (k is a positive integer below n), The result of an operation which performed said predetermined irreversible arithmetic operation to said confidential information n-k times is shown as said presentation information, an approval server means performs said predetermined irreversible arithmetic operation to said presentation information k times, and coincidence with the result of an operation and said collation information is identified.

[Claim 26]An authentication server means to publish an authentication ticket.
An approval server means to which use of an authentication ticket is approved.
A client means which requires an authentication ticket of said authentication server means, and requires use approval of an authentication ticket of said approval server means.
Are the above the authentication method which it had and from an authentication server means to a client means. . Include predetermined irreversible arithmetic operation for n (n is positive integer) time almsgiving ********** in confidential information which an authentication server means and a client means share. The number of times of effective publishes an authentication ticket which is n, and it a client means, Said authentication ticket is shown in an approval server means, ask for use approval, and to a demand of presentation information on an approval server means a client means, When a use count of said authentication ticket is k (k is a positive integer below n), Show the result of an operation which performed said predetermined irreversible arithmetic operation to said confidential information n-k times as said presentation information, and an approval server means, While performing said predetermined irreversible arithmetic operation to said presentation information once and identifying coincidence with the result of an operation and said collation information, collation information included in said authentication ticket is updated to the result of an operation which performed said predetermined irreversible arithmetic operation to said confidential information n-k times.

[Claim 27]Said authentication server means shows a random number to a client means which requires an authentication ticket, requires attestation presentation information, and it a client means, Show the result of an operation which performed said predetermined irreversible arithmetic operation to connection by user

authentication information and said random numbers once [n+] as said attestation presentation information, and an authentication server means, Said predetermined irreversible arithmetic operation is performed to connection by user authentication information currently held and said random numbers once [n+], If coincidence with the result of an operation and said attestation presentation information is checked, the result of an operation which performed said predetermined irreversible arithmetic operation to connection by said user authentication information and said random numbers once will be made into said confidential information, The authentication method according to claim 25 or 26 publishing an authentication ticket which includes n (n is positive integer) time almsgiving ****** collation information for predetermined irreversible arithmetic operation in this.

[Claim 28]Said authentication server means shows a random number to a client means which requires an authentication ticket, requires attestation presentation information, and it a client means, An EXCLUSIVE-OR-operation result of what performed said predetermined irreversible arithmetic operation to connection by user authentication information and said random numbers once or more, and a random number for attestation which a client means generated is shown as said attestation presentation information, An authentication server means counts said random number for attestation backward from said attestation presentation information using user authentication information currently held and said random number, and makes said random number for attestation said confidential information, The authentication method according to claim 25 or 26 publishing an authentication ticket which includes n (n is positive integer) time almsgiving ****** collation information for predetermined irreversible arithmetic operation in this.

[Claim 29]An authenticating processing program recording medium which recorded a processing program of an authentication method performed by the authentication system according to any one of claims 1 to 24, or the authentication method according to any one of claims 25 to 28 in form which an electronic computer can read.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]. This invention permits access of multiple times with one processing in which the validity of a client apparatus accessing a server apparatus is judged. Cipher processing in a client apparatus is made unnecessary, and it enables it to process also with a device with low computation capability especially about single sign-on type an authentication method and an authentication system.

[0002]

[Description of the Prior Art]In recent years, the server client type system which comprises the server apparatus and client apparatus which were connected via the network is general with development of digital communication technique. In such a server client type system, it is important that it checks that a client apparatus and its user have the just authority to access a server apparatus, and unjust access is made not to be performed. Although what is depended on password input is well known as an authentication method which checks this access permission, While the method of asking for password input whenever it accesses is safe, since it is inconvenient, for a user, a single sign-on [which raised convenience] type authentication method has come to be used. Generally as such a single sign-on type authentication method, TTP (Trusted Third-party Protocol) used by a Kerberos authentication system is known, for example.

[0003]Hereafter, it explains, referring to drawings for a conventional single sign-on type authentication method. Drawing 23 is a key map showing the outline of a conventional single sign-on type authentication method, and drawing 24 is a protocol sequence diagram showing a protocol. In drawing 23 and drawing 24, they are a client means in which 81 has a user interface, an authentication server means by which 82 performs user authentication, and an approval server means which 83 judges an access permission and performs use approval.

[0004]In the user authentication procedure of the client means 81 and the authentication server means 82, The client means 81 sends authentication demand Authenticate Request801 which became also considering the user-identification child UID inputted via the user interface, and the server identifier SID as attestation presentation information to the authentication server means 82, On the other hand, the authentication server means 82 returns authentication reply Authorize Request802 accompanied by session key SK enciphered considering the password PW as a key with authentication ticket Ticket803.

[0005]In the use approval procedure of the client means 81 and the approval server means 83, Approval demand Authorize Request804 which became also considering the user-identification child UID as whom the client means 81 was enciphered by session key SK, and the time stamp TSk as presentation information is sent to the approval server means 83 with authentication ticket Ticket805, On the other hand, the approval server means 83 verifies the presentation information and authentication ticket Ticket805 in authentication demand Authorize Request804, and if it admits being just, it will return notice Resultof approval806.

[0006]It explains in a conventional single sign-on type authentication method with the above protocol sequences, referring to drawing 25 for the composition below. Drawing 25 is a functional block diagram showing the composition of a conventional single sign-on type authentication method. Also in drawing 25, they are a client means in

which 81 has a user interface, an authentication server means by which 82 performs user authentication, and an approval server means which 83 judges an access permission and performs use approval.

[0007]The 1st transmission and reception means 311 in which the client means 81 transmits and receives data, The input means 811 which obtains the input from a user, and the session key decoding means 812 which decodes the received session key, The ticket holding mechanism 314 holding the received authentication ticket, and the processing selecting means 315 which chooses processing according to the holding state of an authentication ticket, the secret memory measure 316 which memorizes the decoded session key in secrecy, and the proof which clocks time -- a time check -- it comprises the means 813 and the certification information cryptographer stage 814 which enciphers attested certification information using a session key.

[0008]The 2nd transmission and reception means 321 in which the authentication server means 82 transmits and receives data, the attestation which clocks time -- a time check -- with the means 322 and the authentication information storage means 323 in which the user authentication information of a password etc. was accumulated. It comprises the session key creating means 821 which generates an encryption key for every user authentication processing, the session key cryptographer stage 822 which enciphers a session key using a password, and the ticket cryptographer stage 823 which enciphers an authentication ticket using a session key.

[0009]The 3rd transmission and reception means 331 in which the approval server means 83 transmits and receives data, the approval which clocks time -- a time check -- with the means 332 and the ticket decoding means 831 which decodes an authentication ticket. The ticket effective judging means 832 which performs the validity judging of an authentication ticket, It comprises the approval collation means 835 which carries out comparative collation of the certification information decoding means 833 which decrypts attested certification information, the certification information effective judging means 834 which performs the validity judging of attested certification information, and the contents of the authentication ticket and the contents of attested certification information.

[0010]It explains in the conventional single sign-on type authentication method constituted as mentioned above, referring to drawing 26 for the operation below. First, in the client means 81, The user-identification child UID who shows the user itself, the password PW for user authentication beforehand registered into the authentication server means 82, and the server identifier SID of the object which obtains use approval are inputted into the input means 811 as the user input 800 (ST3101, ST8101). The input means 811 takes out the server identifier 3101, and sends it to the ticket holding mechanism 314 while it holds the user input 800 temporarily. The ticket holding mechanism 314 searches the authentication ticket data corresponding to the server identifier 3101 (ST3102), and sends the notice 3102 of search results to the

processing selecting means 315. When the notice 3102 of search results shows non-**, the processing selecting means 315, When the user authentication processing starting information 8101 is sent to said input means 811 and owner ** is shown, the use approval procedure starting information 8102 is sent to said ticket holding mechanism 314, the secret memory measure 316, and the certification information cryptographer stage 814 (ST3103).

[0011]If the user authentication starting information 8101 is given, said input means 811, The group 8103 of the user-identification child and server identifier which were taken out from the user input 800 held temporarily is sent to the authentication server means 82 as authentication demand Authenticate Request801 via the 1st transmission and reception means 311 (ST8102), The user-identification child 8104 is seen off in the certification information cryptographer stage 814, and the password 8105 is sent to the session key decoding means 812.

[0012]In the authentication server means 82, authentication demand Authenticate Request801 is received by the 2nd transmission and reception means 321, The taken-out user-identification child 8201 is seen off in the authentication information storage means 323 and the ticket cryptographer stage 823, and the server identifier 8202 is sent to the ticket cryptographer stage 823 (ST8201). The authentication information storage means 323 searches the password corresponding to the user-identification child 8201 (ST8202), In being, it sends the password 8203 to the session key cryptographer stage 822, and the notice 8204 of search results is sent to the session key creating means 821 and the session key cryptographer stage 822 (ST8203). When the notice 8204 of search results shows owner **, the session key creating means 821 newly generates the random session key 8205, and sends it to the session key cryptographer stage 822 and the ticket cryptographer stage 823 (ST8204). When the notice 8204 of search results shows owner **, the session key cryptographer stage 822, The encryption session key 8206 which enciphered the session key 8205 using the password 8203 is generated (ST8205), This is sent to the client means 81 as authentication reply Authenticate Response802 via the 2nd transmission and reception means 321 (ST8207). attestation -- a time check -- the means 322 has clocked current time.

The time stamp 3212 based on current time is supplied to the ticket cryptographer stage 823.

Hold the ticket cryptographer stage 823 inside and the server common key corresponding to the server identifier 8202 is used, The authentication ticket data 8207 which enciphered the user-identification child 8201, the server identifier 8202, the time stamp 3212, and the session key 8205 is generated (ST8202, ST8206), This is sent to the client means 81 as authentication ticket Ticket803 via the 2nd transmission and reception means 321 (ST8207).

[0013]In the client means 81, authentication reply Authenticate Response802 is sent

to the session key decoding means 812 as the encryption session key 8106 via the 1st transmission and reception means 311, Authentication ticket Ticket803 is sent to said ticket holding mechanism 314 as the authentication ticket data 8108 via the 1st transmission and reception means 311 (ST8103). Said ticket holding mechanism 314 matches the authentication ticket data 8108 with the server identifier 3101, and holds it (ST3112). The session key decoding means 812 decrypts the encryption session key 8106 using the password 8105 (ST8104). Therefore, only when a right password is entered, a right session key can be obtained. The session key 8107 obtained by the session key decoding means 812 is sent to the secret memory measure 316, and is memorized.

[0014]The secret memory measure 316 sends the memorized session key 8109 to the certification information cryptographer stage 814, when the session key 8107 is memorized in secrecy, only predetermined access is permitted and the use approval procedure starting information 8102 is given (ST8105). proof -- a time check -- the means 813 has clocked current time.

The time stamp 8110 based on current time is supplied to the certification information cryptographer stage 814.

If the use approval procedure starting information 8102 is given, the certification information cryptographer stage 814, The attested certification information 8111 which enciphered the user-identification child 8104 and the time stamp 8110 using the session key 8109 is generated (ST8106), This is sent to the approval server means 83 as approval demand Authorize Request804 via the 1st transmission and reception means 311 (ST8107). If the use approval procedure starting information 8102 is given, said ticket holding mechanism 314, The held authentication ticket data 8112 corresponding to the server identifier 3101 is sent to the approval server means 83 as authentication ticket Ticket805 via the 1st transmission and reception means 311 (ST8107).

[0015]In the approval server means 83, approval demand Authorize Request804 is sent to the certification information decoding means 833 as the attested certification information 8308 via the 3rd transmission and reception means 331, Authentication ticket Ticket805 is sent to the ticket decoding means 831 as the authentication ticket data 8301 via the 3rd transmission and reception means 331 (ST8301). The ticket decoding means 831 decrypts the authentication ticket data 8301 using the self-server common key held inside, The user-identification child 8302 and the server identifier 8303 which were obtained, and the time stamp 8304 are sent to the ticket effective judging means 832, and the session key 8305 is sent to the certification information decoding means 833 (ST8302). approval -- a time check -- the means 332 has clocked current time.

The current time information 8306 is supplied to the ticket effective judging means 832 and the certification information effective judging means 834.

While the ticket effective judging means 832 performs the coincidence decision of the server identifier 8303 and the self-server identifier held inside, It confirms that the difference of the time stamp 8304 and the current time information 8306 is within the limits of the predetermined term of validity, and when all are truth, the user-identification child 8302 is made into the ticket user-identification child 8307, and is seen off in the approval collation means 835 (ST3306, ST3307). The user-identification child 8309 and the time stamp 8310 which were produced by the certification information decoding means 833 decrypting the attested certification information 8308 using the session key 8305 are sent to the certification information effective judging means 834 (ST8303). Since attested certification information is enciphered using the session key by the client means, only when a right session key is used by a client means, a right user-identification child and a time stamp are obtained here. The certification information effective judging means 834 confirms that the difference of the time stamp 8310 and the current time information 8306 is within the limits of a predetermined time lag, When it is truth, the user-identification child 8309 is made into the proof user-identification child 8311, and is seen off in the approval collation means 835 (ST8304, ST8305). The approval collation means 835 performs the coincidence decision of the ticket user-identification child 8307 and the proof user-identification child 8311 (ST8306), If it is truth, the notice 8312 of approval will be sent to the client means 81 as notice Resultof approval806 via the 3rd transmission and reception means 331 (ST8307, ST3317), and it is received in the client means 81 (ST3118). When a coincidence decision becomes truth at this time, the user-identification child and the time stamp are obtained correctly, This shows that the right session key was used by the client means, and since this means that the right password was entered, a user authentication result and its use approval result will correspond.

[0016]

[Problem(s) to be Solved by the Invention]However, since cipher processing which needs great computational complexity in the above-mentioned conventional composition is used abundantly and it is necessary to perform cipher processing at every use approval processing by a client side especially, When client sides were a personal digital assistant and a device with low computation capability like a smart phone, it had the technical problem that it was difficult to perform use approval processing by practical processing time.

[0017]Since the use count of one authentication ticket is not restricted in the above-mentioned conventional composition but it is only having provided the term of validity, Even if the code of the authentication ticket intercepted by the third party should have been decoded and unjust access was performed, it also had the technical problem that a possibility of finishing without being discovered was high.

[0018]This invention solves such a conventional technical problem.

The purpose does not need cipher processing in a client side, but even if it is a device with low computation capability, use approval processing can be performed by practical processing time, It is providing single sign-on type the authentication method and authentication system which can manage the use count of an authentication ticket easily.

[0019]

[Means for Solving the Problem]A client means which this invention holds an authentication ticket whose number of times of effective is n (n is a positive integer) to the 1st, shows this, and asks for use approval in order to solve this technical problem, Compare with said authentication ticket, in response, require presentation information, provide with an approval server means which carries out use approval, and said authentication ticket, He is given by attestation child including a ticket identifier, collation information, the number of times of effective, the time of the date of issue, and a server identifier, and said collation information, Predetermined irreversible arithmetic operation is performed to confidential information which a publisher and said client means of said authentication ticket share n times, Said presentation information in case a use count of said authentication ticket is k (k is a positive integer below n) is characterized by performing said predetermined irreversible arithmetic operation to said confidential information n-k times.

[0020]Single sign-on type an authentication method and an authentication system which cannot need cipher processing in a client side, but can manage a use count of an authentication ticket easily by this, and can eliminate double use are obtained.

[0021]Said authentication server means generates a random number in a user authentication procedure, and this is shown in the 2nd, require attestation presentation information of a client means, and said confidential information, Said predetermined irreversible arithmetic operation is performed to connection by said user authentication information and said random numbers once or more, and said attestation presentation information is characterized by performing said predetermined irreversible arithmetic operation to said confidential information n times.

[0022]thereby -- the above-mentioned effect -- in addition, cipher processing in a client side is not needed in a user authentication procedure, and also single sign-on type an authentication method and an authentication system which can communalize data processing of attestation presentation information and data processing of presentation information are obtained.

[0023]Said authentication server means generates a random number in a user authentication procedure, and this is shown in the 3rd, require attestation presentation information of a client means, and said attestation presentation information, It is an EXCLUSIVE-OR-operation result of what performed said

predetermined irreversible arithmetic operation to connection by said user authentication information and said random numbers once or more, and a random number for attestation which a client means generated, and said confidential information is characterized by being said random number for attestation counted backward from said attestation presentation information.

[0024]Thereby, it adds to the above-mentioned effect, and since collation information included in an authentication ticket becomes unrelated to user authentication information, single sign-on type a safer authentication method and an authentication system which even a possibility that user authentication information will be guessed does not have are obtained from an authentication ticket.

[0025]It is characterized by on the other hand said predetermined irreversible arithmetic operation being tropism hash operation the 4th.

[0026]Thereby, in addition to the above-mentioned effect, even if a client side is a device with low computation capability, single sign-on type an authentication method and an authentication system which can perform use approval processing by practical processing time are obtained.

[0027]To the 5th, said authentication ticket including a publisher identifier said approval server means, While carrying out use approval, update collation information of said authentication ticket, the number of times of effective, the time of the date of issue, a publisher identifier, and an attestation child, and said collation information, It is what performed said predetermined irreversible arithmetic operation to said confidential information n-k times, and is updated, and said number of times of effective is characterized by being updated by n-k.

[0028]Since it is updated in addition to the above-mentioned effect by this whenever it uses an authentication ticket, especially a time stamp is updated and the term of validity in an effective judging can be set up shorter, Single sign-on type an authentication method and an authentication system which possibility of an unauthorized use by a third party can be made smaller, and can shorten response time of use approval further are obtained.

[0029]To the 6th, said client means has managed a use count of said authentication ticket, It is what shows this and asks for use approval with said authentication ticket, Have an authentication ticket management tool which manages a use count of two or more preparations and said authentication ticket for said approval server means, and said authentication server means, While publishing said authentication ticket, point to shelf registration of said authentication ticket to said authentication ticket management tool, and said approval server means, When it points to renewal of a history of said authentication ticket to said authentication ticket management tool in response to presentation of said authentication ticket and a rejected note is received from said authentication ticket management tool, it is characterized by not carrying out use approval.

[0030]thereby -- the above-mentioned effect -- in addition, in a system by which an authentication ticket is not updated, since it becomes possible to use an authentication ticket in common to two or more approval servers, single sign-on type an authentication method and an authentication system with higher convenience are obtained.

[0031]To the 7th, said client means has managed a use count of said authentication ticket, With said authentication ticket, this is shown, ask for use approval, and said approval server means two or more preparations and said authentication server means, Memorize an issuance history, while publishing said authentication ticket, and said approval server means, Memorize an update history, while updating said authentication ticket, and it refers for a history of said authentication ticket to said authentication server means which a publisher identifier of said authentication ticket shows in response to presentation of said authentication ticket, or said approval server means, When a rejected note is received from said authentication server means or said approval server means, it is characterized by not carrying out use approval.

[0032]thereby -- the above-mentioned effect -- in addition, in a system by which an authentication ticket is updated, since the decentralized administration of the use of an authentication ticket can be carried out, single sign-on type an authentication method and an authentication system which can lessen one management resource more are obtained.

[0033]

[Embodiment of the Invention]Hereafter, it explains, referring to drawings for an embodiment of the invention.

[0034](A 1st embodiment) The authentication system of a 1st embodiment comprises the client means 1 with a user interface, an authentication server means 2 to perform user authentication, and the approval server means 3 that judges the access permission of the client means 1 and performs use approval, as shown in drawing 1. Can use a general purpose computer, a Personal Digital Assistant, a smart phone, etc. for the client means 1, for example, and for the authentication server means 2. For example, a general purpose computer, an exclusive authentication server device, etc. can be used, and a general purpose computer, an exclusive approval server apparatus, an exclusive information providing device, etc. can be used for the approval server means 3.

[0035]It is connected by a cable or the wireless communication network between the client means 1 and the approval server means 3. Although not necessarily connected between the client means 1 and the authentication server means 2 in a communication network, it is necessary to share the confidential information 4. As this confidential information 4, a password, a common key system encryption key, or the calculated value computed from them is used, for example.

[0036]The client means 1 holds the authentication ticket 5 used in a use approval procedure. The authentication server means 2 publishes this to the client means 1, and the authentication server means 2 makes collation information the result of having performed irreversible arithmetic operation f to the confidential information 4 n times (n is the number of times of effective of an authentication ticket), adds an attestation child to this, and generates the authentication ticket 5. An attestation child is added for the purpose of the prevention from an alteration of an authentication ticket, and a publisher's proof, and can use a message authorization code, a digital signature, etc.

[0037]In the use approval procedure of the client means 1 and the approval server means 3, the result to which the client means 1 performed irreversible arithmetic operation f to the confidential information 4 in the n−k time (k is a use count in the use approval procedure of an authentication ticket) is used as the presentation information 6. As long as the irreversible arithmetic operation f has sufficiently safe irreversibility, the length of a result, and random nature, since the third party who does not know the confidential information 4 cannot calculate this presentation information 6, it is shown that it is a valid user which gets to know the confidential information 4 using this presentation information 6. Since many number of times of the irreversible arithmetic operation f in presentation information is performed so that it went back in the past and the following presentation information is also incalculable from this presentation information 6, there is also no necessity for encryption.

[0038]Send the client means 1 to the approval server means 3 with the authentication ticket 7 currently held, and this presentation information 6 to this the approval server means 3, A check in agreement with the collation information which the authentication ticket 7 includes is performed, and the result of having carried out irreversible arithmetic operation f to the presentation information 6 k times with an attestation child's verification which the authentication ticket 7 includes will return the notice 8 of approval, if it admits being just.

[0039]By this method, the client means 1 can obtain use approval to n times using the authentication ticket 7, without revealing the confidential information 4 to a third party including the approval server means 3.

[0040]Thus, the authentication system of this embodiment is provided with the following.

The client means which the number of times of effective holds the authentication ticket which is n (n is a positive integer), shows this, and asks for use approval.

The approval server means which requires presentation information in response, compares with said authentication ticket, and carries out use approval.

[0041]Information, including a server identifier etc., other than collation information can be included in said authentication ticket at the time of a ticket identifier, the

number of times of effective, and the date of issue, and an attestation child is given to this. Collation information is information which performed predetermined irreversible arithmetic operation to the confidential information which the publisher and client means of an authentication ticket share n times. Said presentation information is information which performed predetermined irreversible arithmetic operation to said confidential information n-k times, when the use count of an authentication ticket is k (k is a positive integer below n).

[0042]Single sign-on type the authentication method and authentication system which cannot need cipher processing in a client side, but can manage the use count of an authentication ticket easily, and can eliminate double use by such composition are obtained.

[0043](A 2nd embodiment) In the authentication system of a 2nd embodiment, a client means shows attestation presentation information to the authentication server means 22, and requires an authentication ticket.

[0044]The client means 11 in which this authentication system has a user interface as shown in drawing 2, An authentication server means 12 to perform user authentication, and the approval server means 3 which judges the access permission of the client means 11 and performs use approval are comprised, and it is connected by the cable or the wireless communication network between the client means 11, the authentication server means 12, and the approval server means 3. This approval server means 3 is the same as that of a 1st embodiment (drawing 1), there is, and again, The authentication ticket returned to the client means 11 from the authentication server means 12, It is the same as that of a 1st embodiment (drawing 1) also about the presentation information which the client means 11 transmits to the approval server means 3 and an approval ticket, and the notice 8 of approval further returned to the client means 11 from the approval server means 3.

[0045]The client means 11 and the authentication server means 12 of this authentication system share the result of having performed irreversible arithmetic operation f to connection by the password PW entered via the user interface, and the random numbers R obtained from the authentication server means 12 once, as the confidential information 14. As long as the irreversible arithmetic operation f has sufficiently safe irreversibility, the length of a result, and random nature, the third party who does not know the password PW cannot calculate this confidential information 14.

[0046]In the user authentication procedure of the client means 11 and the authentication server means 12, the authentication server means 12 generates a random number, this is shown, and attestation presentation information is required of the client means 11. The client means 11 computes the confidential information 14 by performing irreversible arithmetic operation f to connection by the random numbers R obtained from the password PW and the authentication server means 12 once, It

sends to the authentication server means 12 by making into the attestation presentation information 13 the result of having performed irreversible arithmetic operation f to this confidential information 14 further n times (n+1 total and n are the number of times of effective of an authentication ticket).

[0047]On the other hand, a check of that the confidential information 14 of the authentication server means 12 corresponds from the attestation presentation information 13 will return the authentication ticket 5 which added the attestation child to this by making into collation information the result of having performed irreversible arithmetic operation f to the confidential information 14 n times. The client means 11 is held in order to use this in a use approval procedure. An attestation child is added for the purpose of the prevention from an alteration of an authentication ticket, and a publisher's proof, and can use a message authorization code, a digital signature, etc.

[0048]In the use approval procedure of the client means 11 and the approval server means 3, the result to which the client means 11 performed irreversible arithmetic operation f to the confidential information 14 in the n-k time (k is a use count in the use approval procedure of an authentication ticket) is used as the presentation information 6. As long as the irreversible arithmetic operation f has sufficiently safe irreversibility, the length of a result, and random nature, since the third party who does not know the confidential information 14 cannot calculate this presentation information 6, it is shown that it is a valid user which gets to know the confidential information 14 using this presentation information 6. Since many number of times of the irreversible arithmetic operation f in presentation information is performed so that it went back in the past and the following presentation information is also incalculable from this presentation information 6, there is also no necessity for encryption.

[0049]Verification of the attestation child who sends the client means 11 to the approval server means 3 with the authentication ticket 7 holding this presentation information 6 and in whom the authentication ticket 7 includes the approval server means 3 to this, The result of having carried out irreversible arithmetic operation f to the presentation information 6 k times performs a check in agreement with the collation information which the authentication ticket 7 includes, and if it admits being just, the notice 8 of approval will be returned.

[0050]By this method, the client means 11 can obtain use approval to n times using the authentication ticket 7, without revealing the confidential information 14 and the password PW to a third party including the approval server means 3.

[0051]Thus, in the authentication system of this embodiment, an authentication server means generates a random number in a user authentication procedure, shows this, and requires attestation presentation information of a client means. As confidential information at this time, what performed predetermined irreversible arithmetic operation to connection by user authentication information and random numbers once or more is used, and what performed predetermined irreversible

arithmetic operation to this confidential information n times as attestation presentation information is shown.

[0052]such composition -- the effect of a 1st embodiment -- in addition, also in a user authentication procedure, cipher processing in a client side is unnecessary, and single sign-on type the authentication method and authentication system which can communalize data processing of attestation presentation information and data processing of presentation information are obtained.

[0053](A 3rd embodiment) As shown in drawing 3, the random number for attestation generated by the client means 21 is shared between the client means 21 and the authentication server means 22 as the confidential information 24 by the authentication system of a 3rd embodiment.

[0054]In this system, in a user authentication procedure, the authentication server means 22 generates a random number, this is shown, and attestation presentation information is required of the client means 21. The client means 21 is sent to the authentication server means 22 by making into the attestation presentation information 23 the exclusive OR result of the result of having performed irreversible arithmetic operation f to connection by the random numbers R obtained from the password PW and the authentication server means 22 once, and the confidential information 24 which the client means 21 generated in secrecy. In drawing 3, the sign "@" shows the exclusive OR (EXOR) operation.

[0055]On the other hand, the authentication server means 22 is counted backward from the attestation presentation information 23, the password PW, and the random number R, and asks for the confidential information 25. And irreversible arithmetic operation f is performed to this confidential information 25 n times, that result of an operation is made into collation information, and the authentication ticket 5 which added the attestation child to this is returned to the client means 21. The client means 21 is held in order to use this in a use approval procedure.

[0056]Supposing the attestation presentation information 23 is suitably made from a third party with an inaccurate user, Even if it can obtain the authentication ticket 5 by the client means 21, the client means 21 does not understand the confidential information 25 which the server counted backward using the password PW and the random number R from the attestation presentation information 23. Therefore, the unjust access can be eliminated in a following use approval procedure.

[0057]In the use approval procedure of the client means 21 and the approval server means 3, the result to which the client means 21 performed irreversible arithmetic operation f to the confidential information 24 in the n-k time (k is a use count in the use approval procedure of an authentication ticket) is used as the presentation information 6. As long as the irreversible arithmetic operation f has sufficiently safe irreversibility, the length of a result, and random nature, since the third party who does not know the confidential information 24 cannot calculate this presentation

information 6, it is shown that it is a valid user which gets to know the confidential information 24 using this presentation information 6. Since many number of times of the irreversible arithmetic operation f in presentation information is performed so that it went back in the past and the following presentation information is also incalculable from this presentation information 6, there is also no necessity for encryption.

[0058]Verification of the attestation child who sends the client means 21 to the approval server means 3 with the authentication ticket 7 holding this presentation information 6 and in whom the authentication ticket 7 includes the approval server means 3 to this, The result of having carried out irreversible arithmetic operation f to the presentation information 6 k times performs a check in agreement with the collation information which the authentication ticket 7 includes, and if it admits being just, the notice 8 of approval will be returned.

[0059]By this method, the client means 21 can obtain use approval to n times using the authentication ticket 7, without revealing the confidential information 24 and the password PW to a third party including the approval server means 3.

[0060]Thus, in the authentication system of this embodiment, an authentication server means generates a random number in a user authentication procedure, shows this, and requires attestation presentation information of a client means. Attestation presentation information is an EXCLUSIVE-OR-operation result of what performed predetermined irreversible arithmetic operation to connection by user authentication information and said random numbers once or more, and the random number for attestation (confidential information) which the client means generated, and this confidential information is counted backward from attestation presentation information by an authentication server means.

[0061]By such composition, the collation information which an authentication ticket includes becomes unrelated to user authentication information. Therefore, single sign-on type a safe authentication method and authentication system are obtained rather than even a possibility that user authentication information will be guessed from an authentication ticket cannot be found.

[0062](A 4th embodiment) A 4th embodiment explains the block configuration of each means to perform the concrete communication procedure and it in the authentication system of a 2nd embodiment.

[0063]Drawing 4 is a protocol sequence diagram showing the protocol in this system. In drawing 4, the client means in which 31 has a user interface, an authentication server means by which 32 performs user authentication, and the approval server means which 33 judges an access permission and performs use approval are shown, and the sign "S (K|-)" shows the attestation child attachment function which used the key K.

[0064]In the user authentication procedure of the client means 31 and the authentication server means 32, First, the client means 31 sends authentication

demand Authenticate Request301 accompanied by the user-identification child UID and the server identifier SID which were inputted via the user interface to the authentication server means 32. At this time, authentication demand Authenticate Request301 is good also as a thing accompanied by the number of times n of effective of an authentication ticket. When that is not right, an authentication server shall just define the number of times n of effective fixed.

[0065]On the other hand, the authentication server means 32 returns attestation challenge Challenge302 accompanied by the random number R0 generated so that it might differ each time. The client means 31 which received this returns attestation challenge answer Response303 accompanied by the result of having given n+1 step of hash operation H to connection by the password PW and the random number R0 which were inputted via the user interface, On the other hand, if the authentication server means 32 carries out comparison verification of the n+1-step hash operation result in challenge answer Response303, and the n+1-step hash operation result performed itself and is in agreement, it will admit being just, Authentication ticket Ticket304 to which the attestation child was added with the publisher identifier IID which shows ticket identifier TID and n+1-step hash operation result, time stamp TS0, server identifier SID, and authentication server 32 self is returned. [which were newly generated] The client means 31 is held in order to use this in a use approval procedure.

[0066]In the use approval procedure of the client means 31 and the approval server means 33, the client means 31 sends the approval demand Authorize Request and authentication ticket Ticket305 to the approval server means 33. At this time, the approval demand Authorize Request is good also as a thing accompanied by the user-identification child UID. On the other hand, the approval server means 33 returns approval challenge Challenge306 accompanied by the value k based on the use count of this authentication ticket. The client means 31 which received this returns approval challenge answer Response307 accompanied by the result of having given hash operation [of +one step of n-k] H to connection by the password PW and the random numbers R0.

[0067]Since this hash operation H cannot calculate this hash operation result for the sufficiently safe third party who does not know the password PW and the random number R0 as long as it, on the other hand, has tropism, the length of a result, and random nature, It is shown that it is a valid user which gets to know the password PW by this hash operation result. Since many number of stageses of hash operation H are performed so that it went back in the past and the following hash operation result is also incalculable from this hash operation result, there is also no necessity for encryption. As such hash operation H [like], algorithms, such as MD5 and SHA, can be used, for example.

[0068]On the other hand, the approval server means 32 carries out comparison

verification of the result of having performed hash operation of k stage to the +1 step of n−k hash operation result in approval challenge answer Response307 further, and the n+1−step hash operation result in authentication ticket Ticket, If in agreement, it will admit being just and notice Resultof approval308 will be returned. At this time, the notice 308 of approval is good also as a thing simultaneously accompanied by the information Info to which access was permitted by use approval.

[0069]By the above protocol sequences, the client means 31 can obtain use approval to n times using the authentication ticket 304, without revealing the password PW to a third party including the approval server means 33.

[0070]It explains referring to the functional block diagram of drawing 5 for the composition with such a protocol sequence of an authentication system.

[0071]In drawing 5, they are a client means in which 31 has a user interface, an authentication server means by which 32 performs user authentication, and an approval server means which 33 judges an access permission and performs use approval.

[0072]The client means 31 is provided with the following.

The 1st transmission and reception means 311 that transmits and receives data.

The input means 312 which obtains the input from a user.

A hash means 313 to connect two inputs and to perform hash operation H.

The ticket holding mechanism 314 holding the received authentication ticket, and the processing selecting means 315 which chooses processing according to the holding state of an authentication ticket, A multi stage hash means 317 to perform hash operation of the secret memory measure 316 which memorizes a hash operation result in secrecy, and the given number of stages or the number of stages of the difference of two given numerical values.

[0073]According to the kind of communication network, the 1st transmission and reception means 311 For example, LAN interface devices, such as a LAN card, Telephone interfacing units, such as ISDN interface devices, such as a terminal adopter, and a modem, It is good also as composition which comprises infrared ray interface devices, such as wireless interface devices, such as a portable data communication card and a PIAFS card, and an IrDA module, etc., and uses these some properly according to a communications partner. The input means 312 comprises pointing devices and selection buttons, such as character input devices, such as a keyboard and a ten key, a mouse, a trackball, and a pen tablet, combination of a dial and a display screen, or a touch panel, for example. The hash means 313 is constituted, for example combining a logic circuit and the arithmetic circuit incorporating the algorithm of hash operation H. As for the ticket holding mechanism 314, a memory circuit is used, for example. A logic circuit can be used for the processing selecting means 315, for example. The secret memory measure 316 is

constituted by the memory device which had Tampa-proof nature like an IC card, for example. The multi stage hash means 317 adds the arithmetic circuit etc. which search for the difference of the counter which counts the connection which feeds back an output to the arithmetic circuit which incorporated the algorithm of hash operation H, for example, and a number of stages, or a numerical value, and is constituted. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0074]The authentication server means 32 is provided with the following.

The 2nd transmission and reception means 321 that transmits and receives data.

the attestation which clocks current time -- a time check -- the means 322.

The authentication information storage means 323 which accumulates the user authentication information of a password etc.

The random number generating means 324 which generates a random number for every user authentication processing, and 2nd multi stage hash means 325 by which it is given and reliance also performs hash operation H of many number of stageses one,

The attestation collation means 326 which carries out comparative collation of the two multi stage hash values, the ticket identifier creating means 327 which generates a unique ticket identifier for every authentication ticket issue, and the attestation child addition means 328 which generates and adds the attestation child to an authentication ticket.

[0075]According to the kind of communication network, the 2nd transmission and reception means 321 For example, LAN interface devices, such as a LAN card, It comprises infrared ray interface devices, such as wireless interface devices, such as telephone interfacing units, such as ISDN interface devices, such as a terminal adopter, and a modem, a portable data communication card, and a PIAFS card, and an IrDA module, etc. attestation -- a time check -- as for the means 322, a timer counter is used, for example. If the authentication information storage means 323 is the memory device which comprised a mass memory device and had the Tampa-proof nature, in addition, it is good. The random number generating means 324 comprises an arithmetic circuit which incorporated the random number generation algorithm, for example, or an inverter which data-izes an electromagnetic noise. The 2nd multi stage hash means 325 adds the counter etc. which count the connection which feeds back an output to the arithmetic circuit which incorporated the algorithm of hash operation H, for example, and a number of stages, and is constituted. The attestation collation means 326 comprises a comparison circuit, for example. The ticket identifier creating means 327 comprises a counter circuit which had sufficient bit length, for example. The attestation child addition means 328 comprises the arithmetic circuit and memory

circuit incorporating an attestation child generation algorithm. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0076]The approval server means 33 is provided with the following.

The 3rd transmission and reception means 331 that transmits and receives data.

the approval which clocks current time -- a time check -- the means 332.

The attestation child verifying means 333 which verifies the attestation child added to the authentication ticket.

The ticket effective judging means 334 which performs the validity judging of an authentication ticket, The ticket use management tool 335 which remains with the ticket identifier of an authentication ticket, and the number of times of effective, and manages the number of times of available, the 3rd multi stage hash means 336 that performs hash operation H of the given number of stages, and the approval collation means 337 which carries out comparative collation of the two multi stage hash values.

[0077]According to the kind of communication network, the 3rd transmission and reception means 331 For example, LAN interface devices, such as a LAN card, It comprises infrared ray interface devices, such as wireless interface devices, such as telephone interfacing units, such as ISDN interface devices, such as a terminal adopter, and a modem, a portable data communication card, and a PIAFS card, and an IrDA module, etc. approval -- a time check -- as for the means 332, a timer counter is used, for example. The attestation child verifying means 333 comprises the arithmetic circuit and memory circuit incorporating an attestation child verification algorithm. The ticket effective judging means 334 is constituted by the combination of a comparison circuit, for example. The ticket use management tool 335 is constituted by the combination of the arithmetic circuit which calculates using frequency, and a mass memory device. For example, the 3rd multi stage hash means 336 is a change thing, and the preset value of a counter consists of the same arithmetic circuits as the 2nd multi stage hash means 325. The approval collation means 337 comprises a comparison circuit, for example. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0078]It explains in the authentication method and authentication system which were constituted as mentioned above, referring to drawing 6 for the operation below. Here, the case where authentication demand Authenticate Request301 is accompanied by the number of times n of authentication ticket effective is explained.

[0079]First, in the client means 31, The user-identification child UID who shows the user itself, the password PW for user authentication beforehand registered into the authentication server means 32, the server identifier SID of the object which obtains use approval, and the number of times n of effective of an authentication ticket as the user input 300. It is inputted into the input means 312 (ST3101, ST3104). The input means 312 takes out the server identifier 3101, and sends it to the ticket holding mechanism 314 while it holds the user input 300 temporarily. The ticket holding mechanism 314 searches the authentication ticket data corresponding to the server identifier 3101 (ST3102), and sends the notice 3102 of search results to the processing selecting means 315. When the notice 3102 of search results shows non-**, the processing selecting means 315, The user authentication processing starting information 3103 is sent to said input means 312 and the multi stage hash means 317, and when owner ** is shown, (ST3103) use approval procedure starting information 3104 is sent to said ticket holding mechanism 314, the secret memory measure 316, and the multi stage hash means 317.

[0080]If the user authentication starting information 3103 is given, said input means 312, The group 3105 of the user-identification child and server identifier which were taken out from the user input 300 held temporarily, and the number of times of effective is sent to the authentication server means 32 as authentication demand Authenticate Request301 via the 1st transmission and reception means 311 (ST3105), The number of times 3106 of effective is sent to the multi stage hash means 317, and the password 3107 is sent to the hash means 313.

[0081]In the authentication server means 32, authentication demand Authenticate Request301 is received by the 2nd transmission and reception means 321, The taken-out user-identification child 3201 is seen off in the authentication information storage means 323, the number of times 3202 of effective is sent to the 2nd multi stage hash means 325 and attestation child addition means 328, and the server identifier 3203 is sent to the attestation child addition means 328 (ST3201). The authentication information storage means 323 searches the password corresponding to the user-identification child 3201 (ST3202), In being, it sends (ST3203) and the password 3204 to the 2nd multi stage hash means 325, and the notice 3205 of search results is sent to the random number generating means 324 and the 2nd multi stage hash means 325.

[0082]When the notice 3205 of search results shows owner **, while the random number generating means 324 newly generates the challenge random number 3206 for data disturbance at random and sends it to the 2nd multi stage hash means 325, It sends to the client means 31 as attestation challenge Challenge302 via the 2nd transmission and reception means 321 (ST3204). When the notice 3205 of search results shows owner **, the 2nd multi stage hash means 325, To connection by the password 3204 and the challenge random numbers 3206, from the number of times

3202 of effective, hash operation H of many number of stageses is performed one, and the multi stage hash value 3207 of a result is sent to the attestation collation means 326 (ST3205).

[0083]On the other hand, in the client means 31, it is received by the 1st transmission and reception means 311, the challenge random number 3108 is taken out, and attestation challenge Challenge302 is sent to the hash means 313 (ST3106). The hash means 313 performs hash operation H to connection by the password 3107 and the challenge random numbers 3108 (ST3107), and sends the hash value 3109 of a result to the secret memory measure 316 and the multi stage hash means 317. The secret memory measure 316 memorizes the hash value 3109 in secrecy, and permits only predetermined access, i.e., the renewal of an addition in a user authentication procedure and the reference in a use approval procedure, (ST3108). When the user authentication procedure starting information 3103 is given to the multi stage hash means 317, Hash operation H of the number of stages equivalent to the number of times 3106 of effective is performed to the hash value 3109 (ST3109), and the multi stage hash value 3114 of a result is sent to the authentication server means 32 as attestation challenge answer Response303 via the 1st transmission and reception means 311 (ST3110).

[0084]On the other hand, in the authentication server means 32, it is received by the 2nd transmission and reception means 321, the multi stage hash value 3208 is taken out, and attestation challenge answer Response303 is sent to the attestation collation means 326 (ST3206). The attestation collation means 326 performs the coincidence decision of the multi stage hash value 3207 and the multi stage hash value 3208 (ST3207), While sending the collated result 3209 to the ticket identifier creating means 327, it sends to the attestation child addition means 328 as it is by making the multi stage hash value 3208 into the multi stage hash value 3210. When the collated result 327 shows coincidence, the ticket identifier creating means 327 generates the effective ticket identifier 3212, and sends it to the attestation child addition means 328 (ST3208).

[0085]attestation -- a time check -- the means 322 has clocked current time and supplies the time stamp 3211 based on current time to the attestation child addition means 328. The attestation child addition means 328 connects the publisher identifier which shows ticket identifier 3212, multi stage hash value 3210, number-of-times [of effective] 3202, time stamp 3211, server identifier 3203, and authentication server 32 self, On the other hand, an attestation child is generated and added, and it is considered as the authentication ticket data 3213 (ST3209), and sends to the client means 31 as authentication ticket Ticket304 via the 2nd transmission and reception means 321 (ST3210).

[0086]On the other hand, in the client means 31, it is received by the 1st transmission and reception means 311, the authentication ticket data 3110 is taken out, and

authentication ticket Ticket304 is sent to said ticket holding mechanism 314 (ST3111). Said ticket holding mechanism 314 matches the authentication ticket data 3110 with the server identifier 3101, and holds it (ST3112), passing the 1st transmission and reception means 311 for the authentication ticket data 3111, when the use approval procedure starting information 3104 is given -- as authentication ticket Ticket305 -- the approval demand Authorize Request -- the approval server means 33 -- sending (ST3113). The number of times 3112 of effective is taken out from authentication ticket data, and it sends to the multi stage hash means 317.

[0087]On the other hand, in the approval server means 33, it is received by the 3rd transmission and reception means 331, the authentication ticket data 3301 is taken out, and the approval demand Authorize Request accompanied by authentication ticket Ticket305 is sent to the attestation child verifying means 333 (ST3301). While the attestation child verifying means 333 verifies compatibility with data divisions other than the attestation child of the authentication ticket data 3301, and an attestation child and sends the verification result 3304 to the ticket effective judging means 334 (ST3304), The time stamp 3302 and the server identifier 3303 are taken out from a data division, the ticket identifier 3305, the multi stage hash value 3306, the number of times 3307 of effective, and the publisher identifier 3308 are taken out to the ticket effective judging means 334, and it sends to the ticket use management tool 335, respectively.

[0088]approval -- a time check -- the means 332 has clocked current time and supplies the time stamp 3309 based on current time to the ticket effective judging means 334. When the verification result 3304 shows those without an error, the ticket effective judging means 334 (ST3305), While performing the coincidence decision of the server identifier 3303 and the self-server identifier held inside (ST3302, ST3303), It confirms that the difference of the time stamp 3302 and the time stamp 3309 based on current time is within the limits of the predetermined term of validity (ST3306, ST3307), and when all are truth, the ticket effective notice 3310 is sent to the ticket use management tool 335. If security will improve if this term of validity is set up short, but user convenience falls and is set up for a long time, user convenience will improve, but since security falls, it should take into consideration and define these balance. For example, what is necessary is just to carry out in 12 hours in 8 hours which can cover the office hours on the 1st, if it applies to the business-use system by which severe security is not demanded. however -- the shortest -- the hour corresponding between a client - a server -- and -- each -- a time check -- it can be necessary to cover the time error between means

[0089]When the ticket use management tool 335 has managed the ticket list at this time and the ticket effective notice 3310 is given, it is investigated whether the ticket identifier 3305 is used, under a ticket list is searched, and it is already registered (ST3308). If there is no applicable thing, the group of the number of times 3307 of

effective as a value which remains with the ticket identifier 3305 and the number of times 3307 of effective, and shows the number of times of available will be added to a ticket list, and will be memorized (ST3309, ST3310). At this time, it may memorize in accordance with the multi stage hash value 3306 and the publisher identifier 3308. When there is this added group or a thing applicable by search, it receives that this ** constructs, It asks for the using frequency 3311 which the ticket use management tool 335 remains, reduces the number of times of available one, remains with the number of times of effective, and a difference with the number of times of available shows (ST3311), While sending this to the client means 31 as approval challenge Challenge306 via the 3rd transmission and reception means 331 (ST3312), it sends also to the 3rd multi stage hash means 336. It sends to the approval collation means 337 as it is by making the multi stage hash value 3306 into the multi stage hash value 3312.

[0090]On the other hand, in the client means 31, it is received by the 1st transmission and reception means 311, the using frequency 3115 is taken out, and approval challenge Challenge306 is sent to the multi stage hash means 317 (ST3114). When the use approval procedure starting information 3104 is given, the multi stage hash means 317, The hash value 3113 is obtained from said secret memory measure 316 (ST3115), Hash operation H of the number of stages equivalent to the difference of the number of times 3112 of effective and the using frequency 3115 is performed to the hash value 3113 (ST3116), The multi stage hash value 3116 of a result is sent to the approval server means 33 as approval challenge answer Response307 via the 1st transmission and reception means 311 (ST3117).

[0091]Since hash operation H cannot calculate this multi stage hash value 3116 for the sufficiently safe third party who does not know the password PW and the random number R0 as long as it, on the other hand, has tropism, the length of a result, and random nature, It is shown that it is a valid user which gets to know the password PW by this multi stage hash value 3116. Since many number of stageses of hash operation H in a multi stage hash value are performed so that it went back in the past and the following multi stage hash value is also incalculable from this multi stage hash value 3116, there is also no necessity for encryption. Generally it is supposed 100 or more times [operation / code] that it is hash operation a high speed, and if it is a suitable number of stages, it can process at high speed than the case where a code is used.

[0092]On the other hand, in the approval server means 33, it is received by the 3rd reception means 331, the multi stage hash value 3313 is taken out, and approval challenge answer Response307 is sent to the 3rd multi stage hash means 336 (ST3313). The 3rd multi stage hash means 336 performs hash operation H of the number of stages equivalent to the using frequency 3311 to the multi stage hash value 3313, and sends the secondary multi stage hash value 3314 of a result to the approval collation means 337 (ST3314). The approval collation means 337 performs the

coincidence decision of the multi stage hash value 3312 and the secondary multi stage hash value 3314 (ST3315, ST3316), If it is truth, the notice 3315 of approval will be sent to the client means 31 as notice Resultof approval308 via the 3rd transmission and reception means 331 (ST3317), and it is received in the client means 31 (ST3118). By this method, the client means 31 can obtain use approval to n times using the authentication ticket 305, without revealing the password PW to a third party including the approval server means 33.

[0093]Although it had composition which calculates a multi stage hash value in the client means 31 at every use approval procedure in the above explanation, it is good also as composition which carries out precomputation of the multi stage hash value of all the number of stageses at the time of acquisition of an authentication ticket, and is memorized to the secret memory measure 316. In that case, processing time for every use approval procedure of what needs to use the more nearly mass Tampa-proof nature memory device as the secret memory measure 316 can be shortened more.

[0094]Next, in the authentication system of a 4th embodiment shown in drawing 5, the detailed example of composition and operation of the attestation child addition means 328 at the time of using a message authorization code as an attestation child and the attestation child verifying means 333 are explained with reference to drawing 7 and drawing 8.

[0095]The attestation child addition means 328 is provided with the following.

The self-identifier storage means 328A the identifier which shows the authentication server itself was remembered to be as shown in drawing 7.

Data connecting mechanism 328B which connects data.

A connection data hash means 328C to perform hash operation h.

The server common key memory measure 328D which memorizes the server common key with common authentication server means 31 and approval server means 32 which it has as secret, the common key system cryptographer stage 328E which performs cipher processing of a common key system, and attestation child connecting mechanism 328F which connects an attestation child with data.

[0096]This self-identifier storage means 328A comprises a memory, for example. The data connecting mechanism 328B can consist of logic circuits, for example. The connection data hash means 328C comprises an arithmetic circuit which incorporated the algorithm of hash operation h, for example. Hash operation h may be the same as hash operation H, or may differ here. If the server common key memory measure 328D is the memory device which comprised a memory, for example and had the Tampa-proof nature, in addition, it is good. The common key system cryptographer stage 328E comprises the arithmetic circuit or cipher-processing exclusive processor which incorporated the cryptographic algorithm, for example. As a cryptographic algorithm, DES, Triple DES, etc. can be used here, for example. The attestation child

connecting mechanism 328F comprises a logic circuit, for example.

[0097]The attestation child separating mechanism 333A into which the attestation child verifying means 333 separates an attestation child from data as shown in drawing 8, The 2nd connection data hash means 333B that performs hash operation h, The 2nd server common key memory measure 333C that memorizes the server common key with common authentication server means 31 and approval server means 32 which it has as secret, It provides with the 2nd common key system cryptographer stage 333D that performs cipher processing of a common key system, the data separation means 333E which carries out division separation of the data division, the publisher identifier collation means 333F which compares a publisher identifier, and the comparison means 333G which carries out comparison verification of the message authorization code.

[0098]This attestation child separating mechanism 333A comprises a logic circuit, for example. The 2nd connection data hash means 333B, the 2nd server common key memory measure 333C, and the 2nd common key system cryptographer stage 333D are constituted like 328C, 328D, and 328E in drawing 7, respectively. The data separation means 333E comprises a logic circuit, for example. The publisher identifier collation means 333F comprises a memory circuit and a comparison circuit, for example. The comparison means 333G is constituted by the combination of a comparison circuit, for example. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0099]Operation of the attestation child addition means 328 constituted as mentioned above and the attestation child verifying means 333 is explained. In the attestation child addition means 328, the identifier which shows the authentication server itself to the data connecting mechanism 328B from the self-identifier storage means 328A is first supplied as the publisher identifier 328a. The number of times 3202 of effective and the server identifier 3203 which acquired the data connecting mechanism 328B from the 2nd transmission and reception means 321, the multi stage hash value 3210 obtained from the attestation collation means 326, and attestation -- a time check -- with the time stamp 3211 obtained from the means 322. It arranges and connects in an order that the ticket identifier 3212 obtained from the ticket identifier creating means 327 and the publisher identifier 328a obtained from the self-identifier storage means 328A were able to be defined, and sends to the connection data hash means 328C and the attestation child connecting mechanism 328F as the data division 328b.

[0100]The connection data hash means 328C performs hash operation h to the data division 328b, and sends the hash value 328c of a result to the common key system cryptographer stage 328E. The common key system cryptographer stage 328E

obtains the server common key 328d from the server common key memory measure 328D, uses this for an encryption key, enciphers the hash value 328c, and sends it to the attestation child connecting mechanism 328F as the message authorization code 328e. The attestation child connecting mechanism 328F connects the message authorization code 328e with the data division 328b, and outputs the authentication ticket data 3213.

[0101]In the attestation child verifying means 333, the authentication ticket data 3301 is first inputted into the attestation child separating mechanism 333A, It separates into the message authorization code 333a and the data division 333b, and the message authorization code 333a is sent to the comparison means 333G, and the data division 333b is sent to the 2nd connection data hash means 333B and data separation means 333E, respectively. The 2nd connection data hash means 333B performs hash operation h to the data division 333b, and sends the hash value 333c of a result to the 2nd common key system cryptographer stage 333D. The 2nd common key system cryptographer stage 333D obtains the server common key 333d from the 2nd server common key memory measure 333C, uses this for an encryption key, enciphers the hash value 333c, and sends it to the comparison means 333G as the message authorization code 333e for comparison. While it separates into the time stamp 3302, the server identifier 3303, the ticket identifier 3305, the multi stage hash value 3306, the number of times 3307 of effective, and the publisher identifier 3308 and the data separation means 333E outputs the data division 333b, About the publisher identifier 3308, it sends also to the publisher identifier collation means 333F. The publisher identifier collation means 333F compares whether the publisher identifier 3308 is an identifier of the authentication server 32, and sends 333 f of collated results to the comparison means 333G. The comparison means 333G outputs the verification result 3304 based on whether 333 f of collated results show coincidence, or the message authorization code 333a and the message authorization code 333e for comparison are in agreement. Each that the verification result 3304 shows those without an error is the case of being in agreement.

[0102]Next, in the authentication system of a 4th embodiment of drawing 5, the composition and operation of the attestation child addition means 328 at the time of using a digital signature as an attestation child and the attestation child verifying means 333 are explained with reference to drawing 9 and drawing 10. Differing from drawing 7 in drawing 9 instead of the server common key memory measure 328D and the common key system cryptographer stage 328E, It is in the point of having formed the public key system cryptographer stage 328H which performs cipher processing of the self-secret key memory measure 328G which memorizes the public key system code secret key of authentication server 32 self, and a public key system. If it is the memory device which could use the memory, for example and had the Tampa-proof nature as the self-secret key memory measure 328G, in addition, it is good. As the

public key system cryptographer stage 328H, the arithmetic circuit or cipher-processing exclusive processor which incorporated the cryptographic algorithm, for example can be used. As a cryptographic algorithm, RSA, an elliptic curve cryptosystem, etc. can be used here, for example.

[0103]Differing from drawing 8 in drawing 10 The 2nd server common key memory measure 333C, Instead of the 2nd common key system cryptographer stage 333D and the publisher identifier collation means 333F, The public key system decoding means 333J which performs decoding processing of the server public key accumulation means 333H which matches the public key of the authentication server means 31 with a server identifier, and accumulates it one or more, and a public key system code is established, and it is in the point of having changed connection between these. The server public key accumulation means 333H is good also as what accumulates not only the authentication server means 32 but the public key of the approval server means 33. As the server public key accumulation means 333H, a memory circuit can be used, for example, and if it is a mass memory device, in addition, it is good. As the public key system decoding means 333J, the arithmetic circuit or cipher-processing exclusive processor which incorporated the decoding algorithm, for example can be used. It cannot be overemphasized that the decoding algorithm corresponding to the cryptographic algorithm in the public key system cryptographer stage 328H is used as a decoding algorithm here. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0104]Operation of the attestation child addition means 328 constituted as mentioned above and the attestation child verifying means 333 is explained. In the attestation child addition means 328, the self-identifier storage means 328A, the data connecting mechanism 328B, Operation of the connection data hash means 328C is the same as that of the case of drawing 7, the data division 328b is supplied to the attestation child connecting mechanism 328F, and the hash value 328c is supplied to the public key system cryptographer stage 328H, respectively. The public key system cryptographer stage 328H obtains the self-secret key 328f from the self-secret key memory measure 328G, uses this for an encryption key, enciphers the hash value 328c, and sends it to the attestation child connecting mechanism 328F as 328g of digital signatures. The attestation child connecting mechanism 328F connects 328 g of digital signatures with the data division 328b, and outputs the authentication ticket data 3213.

[0105]In the attestation child verifying means 333, the authentication ticket data 3301 is first inputted into the attestation child separating mechanism 333A, It separates into 333 g of digital signatures, and the data division 333b, and 333 g of digital

signatures are sent to the public key system decoding means 333J, and the data division 333b is sent to the 2nd connection data hash means 333B and data separation means 333E, respectively. The 2nd connection data hash means 333B performs hash operation h to the data division 333b, and sends the hash value of 333 h of a result to the comparison means 333G. While it separates into the time stamp 3302, the server identifier 3303, the ticket identifier 3305, the multi stage hash value 3306, the number of times 3307 of effective, and the publisher identifier 3308 and the data separation means 333E outputs the data division 333b, About the publisher identifier 3308, it sends also to the server public key accumulation means 333H. While the publisher identifier 3308 carries out search collation of whether it is an identifier of the known authentication server 31 (or approval server 32) and sends the collated result 333i to the comparison means 333G, the server public key accumulation means 333H, The server public key 333j corresponding to the publisher identifier 3308 is sent to the public key system decoding means 333J.

[0106]The public key system decoding means 333J uses the server public key 333j for a decode key, decrypts 333 g of digital signatures, and sends them to the comparison means 333G as the hash value 333k for comparison. The comparison means 333G outputs the verification result 3304 based on whether the collated result 333i shows coincidence or the hash value of 333 h and the hash value 333k for comparison are in agreement. Each that the verification result 3304 shows those without an error is the case of being in agreement.

[0107]Thus, when an authentication system takes the composition of this embodiment, even if a client side is a device with low computation capability, it becomes possible to perform use approval processing by practical processing time.

[0108](A 5th embodiment) A 5th embodiment explains the block configuration of each means to perform the concrete communication procedure and it in the authentication system of a 3rd embodiment.

[0109]Drawing 11 is a protocol sequence diagram showing the protocol of the authentication system in a 5th embodiment. It is to differ from drawing 4 in drawing 11 with the client means 41 with a user interface, and an authentication server means 42 to perform user authentication, and the approval server means 33 does not have a change. .Attestation challenge answer Response401 via a user interface. The point accompanied by the exclusive OR result (the sign "@" shows EXCLUSIVE OR operation) of the result of having given 1 step of hash operation H to connection by the password PW and the random number R0 which were inputted, and the random number S0 for attestation which the client means 41 generated in secrecy, Authentication ticket Ticket402, the point that the hash operation result by which 403 is accompanied is a hash operation result of n stage to the random number S0 for attestation, It differs in that the hash operation result by which approval challenge answer Response404 is accompanied is the hash operation of the n-k stage to the

random number S0 for attestation.

[0110]By the above protocol sequences, the client means 41, without revealing the password PW to a third party including the approval server means 33, Use approval can be obtained to n times using the authentication ticket 402, and it does not become even a target of attack for stealing the password PW by an inaccurate third party, since the authentication tickets 402 are contents unrelated to the password PW, but safety is higher.

[0111]It explains referring to the functional block diagram of drawing 12 for the composition with such a protocol sequence of an authentication system.

[0112]Also in drawing 12, an authentication server means 42 to perform the client means 41 and user authentication with a user interface differs from drawing 5, and the approval server means 33 does not have a change. Differing from the client means 31 of drawing 5 in the client means 41 establishes the random number generating means 411 for attestation which generates a random number for every user authentication processing, and the 1st exclusive OR means 412 that performs EXCLUSIVE OR operation for every bit, and it is at the point of having changed a part of connection. Differing from the authentication server means 32 of drawing 5 in the authentication server means 42, Instead of the 2nd multi stage hash means 325 and the attestation collation means 326, The 2nd exclusive OR means 422 that performs EXCLUSIVE OR operation for every 2nd 421 bit hash means that performs hash operation H, and the 2nd multi stage hash means 423 that performs hash operation H of the given number of stages are formed, and it is in the point of having changed a part of connection. As the random number generating means 411 for attestation, the arithmetic circuit which incorporated the random number generation algorithm, for example, or the inverter which data-izes an electromagnetic noise can be used. As the 1st and 2nd exclusive OR means 412 and 422, a logic circuit can be used, for example. As the 2nd hash means 421, the arithmetic circuit which incorporated the algorithm of hash operation H, for example can be used. The counter etc. which count the connection which feeds back an output, for example to the same arithmetic circuit as 421, and a number of stages as the 2nd multi stage hash means 423 can be added and constituted. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0113]It explains referring to drawing 13 for operation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the number of times n of authentication ticket effective is explained.

[0114]First, in the client means 41 and the authentication server means 42, operation of the 1st and 2nd transmission and reception means 311 and 321, the input means

312, the ticket holding mechanism 314, the processing selecting means 315, the authentication information storage means 323, and the random number generating means 324 is the same as that of the case of drawing 5 and drawing 6, It is exchanged in authentication demand Authenticate Request301 and attestation challenge Challenge302, In the client means 41, the number of times 4201 of effective, the server identifier 3203, the password 3204, the notice 4202 of search results, and the challenge random number 3206 are obtained for the user authentication processing starting information 4101 or the use approval procedure starting information 3104 in the authentication server means 42. However, the point that the user authentication processing starting information 4101 is sent to said input means 312, the random number generating means 411 for attestation, and the 1st exclusive OR means 412, The point that the number of times 4201 of effective is sent to the 2nd multi stage hash means 423 and attestation child addition means 328, The point that the notice 4202 of search results is sent to the 2nd hash means 421, random number generating means 324, and ticket identifier creating means 327, While the challenge random number 3206 is sent to the 2nd hash means 421, it differs in that it is sent to the client means 41 via the 2nd transmission and reception means 321.

[0115]Next, in the client means 41 the random number generating means 411 for attestation, If the user authentication processing starting information 4101 is given, the random number 4102 for attestation used for an attested proof will newly be generated at random and in secrecy, and will be sent to the 1st exclusive OR means 412 and secret memory measure 316 (ST4101). The secret memory measure 316 memorizes the random number 4102 for attestation in secrecy, and permits only predetermined access, i.e., the renewal of an addition in a user authentication procedure and the reference in a use approval procedure, (ST4102). If the user authentication processing starting information 4101 is given, the 1st exclusive OR means 412, EXCLUSIVE OR operation for every bit is performed between the hash value 4103 and the random number 4102 for attestation which were obtained from the hash means 313, The disturbance hash value 4104 obtained as a result is sent to the authentication server means 42 as attestation challenge answer Response401 via the 1st transmission and reception means 311 (ST4103, ST4104).

[0116]On the other hand, in the authentication server means 42, it is received by the 2nd transmission and reception means 321, the disturbance hash value 4204 is taken out, and attestation challenge answer Response401 is sent to the 2nd exclusive OR means 422 (ST4202). On the other hand, when the notice 4202 of search results shows owner **, the 2nd hash means 421 performs hash operation H to connection by the password 3204 and the challenge random numbers 3206, and supplies the hash value 4203 of a result to the 2nd exclusive OR means 422 (ST4201). The 2nd exclusive OR means 422 performs EXCLUSIVE OR operation for every bit between the hash value 4203 obtained from the 2nd hash means 421, and the disturbance hash

value 4204, and sends the random number 4205 for attestation obtained as a result to the 2nd multi stage hash means 423 (ST4203). The 2nd multi stage hash means 423 performs hash operation H of a number of stages equivalent to the number of times 4201 of effective to the random number 4205 for attestation, and sends the multi stage hash value 4206 of a result to the attestation child addition means 328 (ST4204).

[0117]the following and ticket identifier creating means 327 and attestation -- a time check -- operation of the means 322 and the attestation child addition means 328, although it is the same as that of the case of drawing 4 and drawing 5, The point of using the notice 4202 of search results instead of the ticket identifier creating means 327 being the collated result 3209, It differs in that the number of times 4201 of effective and the multi stage hash value 4206 are used instead of the attestation child addition means 328 being the number of times 3202 of effective, and the multi stage hash value 3210, The authentication ticket data 4207 of contents which are different in the authentication ticket data 3213 is obtained (ST4205), and it is sent to the client means 41 as authentication ticket Ticket402 via the 2nd transmission and reception means 321.

[0118]On the other hand, in the client means 41, It operates like the case where said 1st transmission and reception means 311 and said ticket holding mechanism 314 are drawing 5 and drawing 6, When the use approval procedure starting information 3104 is given, authentication ticket Ticket403 is sent to the approval server means 33 with the approval demand Authorize Request, and the number of times 3112 of effective is supplied to the multi stage hash means 317.

[0119]Operation of the approval server means 33 for this is the same as that of the case of drawing 5 and drawing 6, and approval challenge Challenge306 is returned.

[0120]On the other hand, in the client means 41, it operates like the case where said 1st transmission and reception means 311 and the multi stage hash means 317 are drawing 5 and drawing 6. However, it is the random number 4105 for attestation which is obtained from said secret memory measure 316 (ST4105), and processing is performed to this. Namely, the multi stage hash means 317 performs hash operation H of the number of stages equivalent to the difference of the number of times 3112 of effective, and the using frequency 3115 (ST4106), The multi stage hash value 4106 of a result is sent to the approval server means 33 as approval challenge answer Response404 via the 1st transmission and reception means 311 (ST4107).

[0121]It is only that the candidate for hash differs between the multi stage hash value by which approval challenge answer Response404 which the approval server means 33 obtains by this is accompanied, and the multi stage hash value by which authentication ticket Ticket403 is accompanied in the case of drawing 5 and drawing 6, and the operation relation between the former and the latter is maintained. Therefore, if operation of the approval server means 33 for this may be the same as that of the case of drawing 5 and drawing 6, checks the relation of two multi stage hash values

and accepts that it is just, notice Resultof approval308 will be returned, and it is received in the client means 41. By this method, without revealing the password PW to a third party including the approval server means 33, the password PW of the client means 41 is unrelated, and it can obtain use approval to n times using the higher authentication ticket 402 of safety.

[0122]Although it had composition which calculates a multi stage hash value in the client means 41 at every use approval procedure in the above explanation, it is good also as composition which carries out precomputation of the multi stage hash value of all the number of stageses at the time of acquisition of an authentication ticket, and is memorized to the secret memory measure 316. In that case, processing time for every use approval procedure of what needs to use the more nearly mass Tampa-proof nature memory device as the secret memory measure 316 can be shortened more.

[0123]Thus, when an authentication system takes the composition of this embodiment, even if a client side is a device with low computation capability, it becomes possible to perform use approval processing by practical processing time. Since the collation information included in an authentication ticket becomes unrelated to user authentication information, a possibility that user authentication information will be guessed disappears from an authentication ticket, and single sign-on type an authentication method and an authentication system with higher safety are obtained.

[0124](A 6th embodiment) In the authentication system of a 6th embodiment, the authentication ticket in which using frequency was updated is sent to a client means with the notice of approval from an approval server.

[0125]Drawing 14 is a protocol sequence diagram showing the protocol of this authentication system. In drawing 14, the client means 51 and the approval server means 53 differ from drawing 4, and the authentication server means 32 does not have a change. It differs in that authentication ticket Ticket501 updated by the client means 51 with notice Resultof approval308 from the approval server 53 is sent.

[0126]This authentication ticket Ticket501 compared with the authentication ticket 305, the following point is different.

[0127]That is, the n+1-step hash operation result in the authentication ticket 305 is transposed to the +1 step of n-k hash operation result (k is using frequency). The number of times n of effective in the authentication ticket 305 remains, and it is transposed to number-of-times n-k of available. Time stamp TS0 is transposed to the new time stamp TSk. The publisher identifier IID is transposed to the server identifier which shows approval server 53 self. A new attestation child is added.

[0128]By this method, the client means 51 can obtain use approval to n times using the authentication ticket 304 or the updated authentication ticket 501, without revealing the password PW to a third party including the approval server means 53. Since the time stamp of an authentication ticket is updated each time, the term of validity can be set up shorter. Therefore, the period which can become a target of

attack by an inaccurate third party becomes short, and safety is higher. Since the number of the hash operations in the approval server means 53 may be one, the response time in a use approval procedure can be shortened.

[0129]It explains referring to drawing 15 for the composition with such a protocol sequence of an authentication system.

[0130]In drawing 15, the client means 51 and the approval server means 53 differ from drawing 5, and the authentication server means 32 does not have a change. Differing from the client means 31 of drawing 5 in the client means 51 has the ticket holding mechanism 511 in the point of having enabled it to also hold the authentication ticket data 5101 of authentication ticket Ticket501 from the approval server means 53. Differing from the approval server means 33 of drawing 5 in the approval server means 53, The ticket use management tool 531 shall remain and the number of times of available shall also be outputted. The 3rd hash means 532 that performs 1 step of hash operation H instead of the 3rd multi stage hash means 336 is formed, the 2nd attestation child addition means 533 that generates and adds the attestation child to an authentication ticket is newly established, and it is in the point of having changed a part of connection.

[0131]As this ticket holding mechanism 511, the same composition as the ticket holding mechanism 314 can add and use connection. As the ticket use management tool 531, the same composition as the ticket use management tool 335 can add and use connection. As the 3rd hash means 532, the arithmetic circuit which incorporated the algorithm of hash operation H, for example can be used. As the 2nd attestation child addition means 533, the same composition as the attestation child addition means 328 can be used. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0132]It explains referring to drawing 16 for operation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the number of times n of authentication ticket effective is explained.

[0133]First, the operation in the client means 51 and the authentication server means 32 is the same as that of the case of drawing 5 and drawing 6, a user authentication procedure is performed and, eventually, authentication ticket Ticket304 is sent to the client means 51 from the authentication server means 32.

[0134]On the other hand, in the client means 51, The 1st transmission and reception means 311 operates like the case of drawing 5 and drawing 6, and the ticket holding mechanism 511 operates like drawing 5 and the ticket holding mechanism 314 in the case of drawing 6, While authentication ticket Ticket305 is sent to the approval server

means 53 with the approval demand Authorize Request, the number of times 3112 of effective is taken out from authentication ticket data, and it is sent to the multi stage hash means 317.

[0135]On the other hand, in the approval server means 53, the 3rd transmission and reception means 331 and approval -- a time check -- the means 332, the attestation child verifying means 333, and the ticket effective judging means 334 operating like the case of drawing 5 and drawing 6, and, The ticket identifier 3305, the multi stage hash value 3306, the number of times 3307 of effective, the publisher identifier 3308, and the ticket effective notice 3310 are supplied to the ticket use management tool 531. The ticket use management tool 531 operates almost like drawing 5 and the ticket use management tool 335 in the case of drawing 6, Although the using frequency 5301 is sent to the client means 51 as approval challenge Challenge306 via the 3rd transmission and reception means 331 and being sent to the approval collation means 337 as it is by making the multi stage hash value 3306 into the multi stage hash value 5302, Furthermore, it remains with a ticket identifier, the group 5303 of the number of times of available and a server identifier is outputted, and it sends to the 2nd attestation child addition means 533.

[0136]Operation of the client means 51 for this is the same as that of the case of drawing 5 and drawing 6, and approval challenge answer Response307 is returned to approval challenge Challenge306.

[0137]On the other hand, in the approval server means 53, it is received by the 3rd transmission and reception means 331, the multi stage hash value 5304 is taken out, and approval challenge answer Response307 is sent to the 3rd hash means 532 and the 2nd attestation child addition means 533. The 3rd hash means 532 performs hash operation H to the multi stage hash value 5304, and sends the secondary multi stage hash value 5305 whose number of stages of hash increased by one to the approval collation means 337 (ST5301). The approval collation means 337 performs the coincidence decision of the multi stage hash value 5302 and the secondary multi stage hash value 5305 (ST5302, ST3316), and sends the collated result 5307 to the 2nd attestation child addition means 533.

[0138]approval -- a time check -- the means 322 has clocked current time and supplies the time stamp 5306 based on current time to the 2nd attestation child addition means 533. The 2nd attestation child addition means 533 connects the publisher identifier which remains with a ticket identifier and shows number-of-times [of available], group [of a server identifier] 5303, multi stage hash value 5304, time stamp 5306, and approval server 53 self, On the other hand, an attestation child is generated and added, and it is considered as the authentication ticket data 5308 (ST5303), and sends to the client means 51 with notice Resultof approval308 as authentication ticket Ticket501 via the 3rd transmission and reception means 331 (ST5304).

[0139]On the other hand, in the client means 51, It is received by the 1st transmission and reception means 311, and authentication ticket Ticket501 is sent to said ticket holding mechanism 511 as the authentication ticket data 5101, is held (ST5101, ST5102), and is used in a next use approval procedure.

[0140]Since the number of stages of the multi stage hash value by which the authentication ticket 305 sent to the approval server means 53 is accompanied decreases every [1] for every use approval and it goes from the client means 51 by this, in the approval server means 53, what is necessary is just to perform one step of hash operation, and it can shorten response time. Since a time stamp is updated, it can set to the shortness of the grade which can cover the interval of access to the term of validity, for example, 1 hour, and the user convenience can improve safety, without making it fall. By this method, the client means 31 can obtain use approval in the shorter response time to n times using the higher authentication ticket 305 of safety, without revealing the password PW to a third party including the approval server means 53.

[0141]Although it had composition which calculates a multi stage hash value in the client means 51 at every use approval procedure in the above explanation, it is good also as composition which carries out precomputation of the multi stage hash value of all the number of stageses at the time of acquisition of an authentication ticket, and is memorized to the secret memory measure 316. In that case, processing time for every use approval procedure of what needs to use the more nearly mass Tampa-proof nature memory device as the secret memory measure 316 can be shortened more.

[0142]Thus, in the authentication system of this embodiment, possibility of the unauthorized use by a third party can be made smaller, and the response time of use approval can be shortened.

[0143](A 7th embodiment) An authentication ticket can be used for the authentication system of a 7th embodiment in common to two or more approval servers.

[0144]Drawing 17 is a protocol sequence diagram showing the protocol of this authentication system. In drawing 17, the client means 61, the authentication server means 62, and the approval server means 63 differ from drawing 4, and it has added the authentication ticket management tool 64 further. .Attestation challenge answer Response303. Authentication ticket shelf registration directions Registration601 accompanied by the ticket identifier TID and the server identifier SID which the received authentication server means 62 took out from authentication demand Authenticate Request301, and the number of times n of effective. The point sent to the authentication ticket management tool 64, the point accompanied by the using frequency k in approval demand Authorize Request602, Approval demand Authorize Request602. Authentication ticket Ticket305 [and]. Authentication ticket history update indication Update603 accompanied by the ticket identifier TID and the server identifier SID which the received approval server means 63 took out from approval

demand Authorize Request602 and the authentication ticket 305, and the using frequency k. The point accompanied by the random number Rk generated so that it might differ each time instead of the point sent to the authentication ticket management tool 64, the point that authentication ticket rejected note Reject606 is returned if needed to this, and approval challenge Challenge604 being the using frequency k, The points accompanied by the result of having carried out EXCLUSIVE OR operation with Rk to the result which approval challenge answer Response605 gave hash operation [of +one step of n-k] H to connection by the password PW and the random numbers R0 further differ.

[0145]By this method, the client means 61, without revealing the password PW to a third party including the approval server means 63, In order to check by the authentication ticket management tool 64 which could obtain use approval to n times using the authentication ticket 304, sent the using frequency k from the client means 61, and became independent in the approval server means 63, The authentication ticket 304 can be made available in common by two or more approval server means 63.

[0146]It explains referring to drawing 18 for the composition with this protocol sequence of an authentication system. Also in drawing 18, the client means 61, the authentication server means 62, and the approval server means 63 differ from drawing 5, and it has added the authentication ticket management tool 64 further. Differing from the client means 31 of drawing 5 in the client means 61, While holding an authentication ticket, the ticket maintenance management tool 611 which manages the using frequency k is established instead of the ticket holding mechanism 314, the 1st exclusive OR means 612 that performs EXCLUSIVE OR operation for every bit is established, and it is in the point of having changed a part of connection. Differing from the authentication server means 32 of drawing 5 in the authentication server means 62 forms a ticket registration instruction means 621 to generate authentication ticket shelf registration indicative data, and it is at the point of having changed a part of connection.

[0147]Differing from the approval server means 33 of drawing 5 in the approval server means 63, The ticket update indication means 631 which generates authentication ticket history update indication data while remaining with the ticket identifier of an authentication ticket and the number of times of effective, receiving the number of times of available and supplying each part is established instead of the ticket use management tool 335, The 2nd exclusive OR means 633 that performs EXCLUSIVE OR operation for every 2nd 632 bit random number generating means that generates a random number for every use approval processing is established, and it is in the point of having changed a part of connection.

[0148]As this ticket maintenance management tool 611, the adder circuit which calculates using frequency is added to the same composition as the ticket holding mechanism 335, and it is constituted. As the 1st and 2nd exclusive OR means 612 and

633, a logic circuit can be used, for example. As the ticket registration instruction means 621, a logic circuit can be used, for example. As the ticket update indication means 631, a logic circuit can be used, for example. As the 2nd random number generating means 632, the same composition as the random number generating means 324 can be used. The combination of the arithmetic circuit and comparison circuit which compare various communication-interface devices, the logic circuit which performs division combination of data, and using frequency as the authentication ticket management tool 64, and a mass memory device can constitute. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0149]It explains referring to drawing 19 for operation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the number of times n of authentication ticket effective is explained.

[0150]First, the operation in the client means 61 in a user authentication procedure and the authentication server means 62 is the same as that of the case of drawing 5 and drawing 6 almost, and authentication ticket Ticket304 is eventually sent to the client means 61 from the authentication server means 62. However, in the client means 61, the ticket maintenance management tool 611 operates the ticket holding mechanism 314 at this time. In the authentication server means 62, the number of times 6201 of effective taken out from authentication demand Authenticate Request301 is sent also to the multi stage hash means 325, and the ticket registration instruction means 621 besides the attestation child addition means 328, The server identifier 6202 is sent to the ticket registration instruction means 621 besides the attestation child addition means 328, and the ticket identifier 6203 generated by the ticket identifier creating means 327 is sent to the ticket registration instruction means 621 besides the attestation child addition means 328.

[0151]The ticket registration instruction means 621 connects the ticket identifier 6203, the server identifier 6202, and the number of times 6201 of effective, and generates the authentication ticket shelf registration indicative data 6204, It sends to the authentication ticket management tool 64 as authentication ticket shelf registration directions Registration601 via the 2nd transmission and reception means 321 (ST6201). It is investigated whether when the ticket list is managed and authentication ticket shelf registration directions Registration601 is given, the authentication ticket management tool 64 which received this uses a ticket identifier, searches under a ticket list, and is already registered. If there is no applicable thing, the group of the number of times of effective as a value which remains with a ticket identifier and the number of times of effective, and shows the number of times of

available will be added to a ticket list, and will be memorized.

[0152]On the other hand, in the client means 61, it is received by the 1st transmission and reception means 311, the authentication ticket data 3110 is taken out, and authentication ticket Ticket304 is sent to the ticket maintenance management tool 611. The ticket maintenance management tool 611 matches the authentication ticket data 3110 with the server identifier 3101, and holds it, Remain and the number of times of effective taken out from authentication ticket data is simultaneously managed as the number of times of available (ST6101), When the use approval procedure starting information 6101 is given, the authentication ticket data 3111 via the 1st transmission and reception means 311 as authentication ticket Ticket305, The using frequency 6102 obtained by lengthening from the number of times of effective taken out from the authentication ticket after remaining and reducing the number of times of available one via the 1st (ST6102) transmission and reception means 311 as approval demand Authorize Request602, It sends to the approval server means 63 (ST6103), and the number of times 3112 of effective taken out from authentication ticket data is further sent to the multi stage hash means 317.

[0153]On the other hand, in the approval server means 63, Authentication ticket Ticket305 and approval demand Authorize Request602 are received by the 3rd transmission and reception means 331, The authentication ticket data 3301 is taken out, it is sent to the attestation child verifying means 333, the using frequency 6301 is taken out, and it is sent to the ticket update indication means 631 (ST6301). approval -- a time check -- the means 332, the attestation child verifying means 333, and the ticket effective judging means 334 operating almost like the case of drawing 5 and drawing 6, and, However, the server identifier 6302 is sent to the ticket update indication means 631 besides the ticket effective judging means 334, and the effective notice 6303 is sent to the ticket update indication means 631 and the 2nd random number generating means 632. If the effective notice 6303 is given, the ticket update indication means 631, Connect the ticket identifier 3305, the server identifier 6302, and the using frequency 6301, and the authentication ticket history update indication data 6304 is generated, passing the 3rd transmission and reception means 331 -- as authentication ticket history update indication Update603 -- the authentication ticket management tool 64 -- sending (ST6302) -- it sends to the 3rd multi stage hash means 336 by making using frequency 6301 into the using frequency 6306 as it is. When authentication ticket history update indication Update603 is given, the authentication ticket management tool 64, The value which searches under a ticket list using a ticket identifier, and shows the corresponding number of times of effective, It is confirmed that it is in agreement with the sum total of the corresponding value which remains and shows the number of times of available, and the using frequency by which authentication ticket history update indication Update603 is accompanied, If right, the value which shows the number of times of remaining available under ticket

list will be reduced one, and if not right, authentication ticket rejected note Reject606 is returned. The authentication ticket rejected note 606 is sent to said ticket update indication means 631 as the authentication ticket rejected note data 6305 via the 3rd transmission and reception means 331 in the approval server means 63. Although the ticket update indication means 631 is sent to the approval collation means 337 as it is by making the multi stage hash value 3306 into the multi stage hash value 3312, if the authentication ticket rejected note data 6305 is given, it will deter this. If the effective notice 6303 is given, while the 2nd random number generating means 632 will newly generate the challenge random number 6307 for data disturbance at random and will send it to the 2nd exclusive OR means 633, It sends to the client means 61 as approval challenge Challenge604 via the 3rd transmission and reception means 331 (ST6303).

[0154]On the other hand, in the client means 61, it is received by the 1st transmission and reception means 311, the challenge random number 6103 is taken out, and approval challenge Challenge604 is sent to the 1st exclusive OR means 612 (ST6104). When the use approval procedure starting information 6101 is given, the multi stage hash means 317, From said secret memory measure 316, the hash value 3113 is obtained, hash operation H of the number of stages which is equivalent to the difference of the number of times 3112 of effective and the using frequency 6102 at the hash value 3113 is performed, and the multi stage hash value 6104 of a result is sent to the 1st exclusive OR means 612. When the use approval procedure starting information 6101 is given, the 1st exclusive OR means 612, EXCLUSIVE OR operation for every bit is performed between the multi stage hash value 6104 and the challenge random number 6103, The disturbance multi stage hash value 6105 is generated, and it sends to the approval server means 63 as approval challenge answer Response605 via the 1st transmission and reception means 311 (ST6105, ST6106). Since hash operation H cannot calculate this disturbance multi stage hash value 6105 for the sufficiently safe third party who does not know the password PW, the random number R0, and a challenge random number as long as it, on the other hand, has tropism, the length of a result, and random nature, It is shown that it is a valid user which gets to know the password PW by this disturbance multi stage hash value 6105. Since many number of stageses of hash operation H in a multi stage hash value are performed so that it went back in the past and the following multi stage hash value is also incalculable from this multi stage hash value 6104, there is also no necessity for encryption. Generally it is supposed 100 or more times [operation / code] that it is hash operation a high speed, and if it is a suitable number of stages, it can process at high speed than the case where a code is used.

[0155]On the other hand, in the approval server means 63, it is received by the 3rd transmission and reception means 331, the disturbance multi stage hash value 6308 is taken out, and approval challenge answer Response605 is sent to the 2nd exclusive

OR means 633 (ST6304). The 2nd exclusive OR means 633 performs EXCLUSIVE OR operation for every bit between the challenge random number 6307 and the disturbance multi stage hash value 6308, obtains the multi stage hash value 6309, and sends it to the 3rd multi stage hash means 336 (ST6305). The 3rd multi stage hash means 336 performs hash operation of the number of stages equivalent to the using frequency 6306 to the multi stage hash value 6309, and sends the secondary multi stage hash value 3314 of a result to the approval collation means 337. The approval collation means 337 operates like the case of drawing 5 and drawing 6, sends the notice data 3315 of approval to the client means 61 as notice Resultof approval308 via the 3rd transmission and reception means 331, and is received in the client means 61. However, it is not this limitation when supply of the multi stage hash value 3312 is deterred by reception of authentication ticket rejected note Reject606 (ST6306, ST6307). By this method, the client means 61 can obtain use approval to two or more approval server means using the authentication ticket 305 to n times, without revealing the password PW to a third party including the approval server means 63.

[0156]Although it had composition which calculates a multi stage hash value in the client means 61 at every use approval procedure in the above explanation, it is good also as composition which carries out precomputation of the multi stage hash value of all the number of stageses at the time of acquisition of an authentication ticket, and is memorized to the secret memory measure 316. In that case, processing time for every use approval procedure of what needs to use the more nearly mass Tampa-proof nature memory device as the secret memory measure 316 can be shortened more.

[0157]Thus, the single sign-on type authentication system with high convenience which can use an authentication ticket in common to two or more approval servers under the method with which an authentication ticket is not updated can consist of this embodiment.

[0158](An 8th embodiment) The authentication system of an 8th embodiment can carry out decentralized administration of the use of an authentication ticket.

[0159]Drawing 20 is a protocol sequence diagram showing the protocol of this authentication system. In drawing 20, the client means 71, the authentication server means 72, and the approval server means 73 differ from drawing 14, and it has added the 2nd [further] approval server means 74. The point accompanied by the using frequency k in approval demand Authorize Request701, Approval demand Authorize Request701. Authentication ticket Ticket305 [and]. Authentication ticket history reference Inquiry702 accompanied by the ticket identifier TID and the server identifier SID which the received approval server means 73 took out from approval demand Authorize Request701 and the authentication ticket 305, and the using frequency k. The point sent to the authentication server means 72 or the 2nd approval server means 74, the point that authentication ticket rejected note Reject705 is returned if needed to this, The point accompanied by the random number Rk generated so that it

might differ each time instead of approval challenge Challenge703 being the using frequency k, The points accompanied by the result of having carried out EXCLUSIVE OR operation with Rk to the result which approval challenge answer Response704 gave hash operation [of +one step of n-k] H to connection by the password PW and the random numbers R0 further differ.

[0160]By this method, the client means 71, without revealing the password PW to a third party including the approval server means 73 and the 2nd approval server means 74, Use approval can be obtained to n times using the authentication ticket 304 or the updated authentication ticket 501, In order to send and check the using frequency k to the authentication server means 72 or the 2nd updated approval server means 74 which published the authentication ticket via the approval server means 73 from the client means 71, The authentication ticket 304 can be made available in common by two or more approval server means 73 and 74, and the traffic of check processing can be decentralized.

[0161]It explains referring to drawing 21 for the composition with such a protocol sequence of an authentication system. Also in drawing 21, the client means 71, the authentication server means 72, and the approval server means 73 differ from drawing 15, and it has added the 2nd [further] approval server means 74. Differing from the client means 51 of drawing 15 in the client means 71, While holding an authentication ticket, the ticket maintenance management tool 711 which manages the using frequency k is established instead of the ticket holding mechanism 511, the 1st exclusive OR means 712 that performs EXCLUSIVE OR operation for every bit is established, and it is in the point of having changed a part of connection. Differing from the authentication server means 32 of drawing 15 in the authentication server means 72 establishes the ticket issue management tool 721 which manages issue of an authentication ticket and is answered to reference, and it is at the point of having changed a part of connection. Differing from the approval server means 53 of drawing 15 in the approval server means 73, The renewal management tool 731 of a ticket which manages renewal of an authentication ticket and is answered to reference while remaining with the ticket identifier of an authentication ticket and the number of times of effective, receiving the number of times of available and supplying each part is established instead of the ticket use management tool 531, The 2nd exclusive OR means 733 that performs EXCLUSIVE OR operation for every 2nd 732 bit random number generating means that generates a random number for every use approval processing is established, and it is in the point of having changed a part of connection. The 2nd approval server means 74 has the same composition as the approval server means 73.

[0162]It can be used as the ticket maintenance management tool 711, being able to add the adder circuit which calculates using frequency to the same composition as the ticket holding mechanism 511. As the 1st and 2nd exclusive OR means 712 and

733, a logic circuit can be used, for example. The combination of the arithmetic circuit and comparison circuit which compare the logic circuit which performs division combination of data, for example, and using frequency as the ticket issue management tool 721, and a mass memory device can constitute. The combination of the arithmetic circuit and comparison circuit which compare the logic circuit which performs division combination of data, for example, and using frequency as the renewal management tool 731 of a ticket, and a mass memory device can constitute. As the 2nd random number generating means 732, the same composition as the random number generating means 324 can be used. Each above-mentioned means may be realized using the computer program on a microcomputer or a general purpose computer. Or it may record on a program recording medium in the form which can read the computer program, and the composition combined with the program-recording-medium reader may realize.

[0163]It explains referring to drawing 22 for operation of the authentication system constituted as mentioned above. Here, the case where authentication demand Authenticate Request301 is accompanied by the number of times n of authentication ticket effective is explained.

[0164]First, the operation in the client means 71 in a user authentication procedure and the authentication server means 72 is the same as that of the case of drawing 15 and drawing 16 almost, and authentication ticket Ticket304 is eventually sent to the client means 71 from the authentication server means 72. However, in the client means 71, the ticket maintenance management tool 711 operates the ticket holding mechanism 511 at this time. In the authentication server means 72, the number of times 7201 of effective taken out from authentication demand Authenticate Request301 is sent to the ticket issue management tool 721 besides the multi stage hash means 325 and the attestation child addition means 328, The server identifier 7202 is sent to the ticket issue management tool 721 besides the attestation child addition means 328, and the ticket identifier 7203 generated by the ticket identifier creating means 327 is sent to the ticket issue management tool 721 besides the attestation child addition means 328. The ticket issue management tool 721 has managed the published ticket list, and the group of the number of times 7201 of effective as a value which remains with the ticket identifier 7203, the server identifier 7202, and the number of times 7201 of effective, and shows the number of times of available is added to a ticket list, and it memorizes it (ST7201).

[0165]On the other hand, in the client means 71, it is received by the 1st transmission and reception means 311, the authentication ticket data 3110 is taken out, and authentication ticket Ticket304 is sent to said ticket maintenance management tool 711. Said ticket maintenance management tool 711 matches the authentication ticket data 3110 with the server identifier 3101, and holds it, Remain and the number of times of effective taken out from authentication ticket data is simultaneously

managed as the number of times of available (ST7101), When the use approval procedure starting information 7101 is given, the authentication ticket data 3111 via the 1st transmission and reception means 311 as authentication ticket Ticket305, The using frequency 7102 obtained by lengthening from the number of times of effective taken out from the authentication ticket after remaining and reducing the number of times of available one via the 1st (ST7102) transmission and reception means 311 as approval demand Authorize Request701, It sends to the approval server means 73, respectively (ST7103), and the number of times 3112 of effective further taken out from authentication ticket data is sent to the multi stage hash means 317.

[0166]On the other hand, in the approval server means 73, Authentication ticket Ticket305 and approval demand Authorize Request701 are received by the 3rd transmission and reception means 331, The authentication ticket data 3301 is taken out, it is sent to the attestation child verifying means 333, the using frequency 7301 is taken out, and it is sent to the renewal management tool 731 of a ticket (ST7301).

[0167]approval -- a time check -- the means 332, the attestation child verifying means 333, and the ticket effective judging means 334 operating almost like the case of drawing 15 and drawing 16, and, However, the server identifier 7302 is sent to the renewal management tool 731 of a ticket besides the ticket effective judging means 334, and the effective notice 7303 is sent to the renewal management tool 731 of a ticket, and the 2nd random number generating means 732. If the published ticket list is managed and the effective notice 7303 is given, the renewal management tool 731 of a ticket, Connect the ticket identifier 3305, the server identifier 7302, and the using frequency 7301, and the authentication ticket history inquiry data 7304 is obtained, While sending authentication ticket history reference Inquiry702 to the authentication server means 72 or the 2nd approval server means 74 which the publisher identifier 3308 shows via the 3rd transmission and reception means 331, The group of the number of times 7301 of effective as a value which remains with the ticket identifier 3305, the server identifier 7302, and the number of times 7301 of effective, and shows the number of times of available is added to a ticket list, and is memorized (ST7302).

[0168]In the authentication server means 72 which received this, it is received by the 2nd transmission and reception means 321, and authentication ticket history reference Inquiry702 is sent to said ticket issue management tool 721 as the authentication ticket history inquiry data 7205 having contained a ticket identifier, a server identifier, and using frequency. The using frequency taken out from the authentication ticket history inquiry data 7205 said ticket issue management tool 721, It investigates whether it is in agreement with what remained with the number of times of effective managed itself, and was added to the difference with the number of times of available one, and in being inharmonious, it returns the authentication ticket rejected note data 7204 as authentication ticket rejected note Reject705 via the 2nd transmission and reception means 321. When the 2nd approval server means 74

receives this, the role as said ticket issue management tool 721 with same renewal management tool of a ticket is performed.

[0169]In the approval server means 73, the authentication ticket rejected note 705 is sent to said renewal management tool 731 of a ticket as the authentication ticket rejected note data 7305 via the 3rd transmission and reception means 331. Although said renewal management tool 731 of a ticket is sent to the approval collation means 337 as it is by making the multi stage hash value 3306 into the multi stage hash value 5302, it remains with a ticket identifier and the group 5303 of the number of times of available and a server identifier is sent to the 2nd attestation child addition means 533, These will be deterred if the authentication ticket rejected note data 7305 is given. If the effective notice 7303 is given, while the 2nd random number generating means 732 will newly generate the challenge random number 7306 for data disturbance at random and will send it to the 2nd exclusive OR means 733, It sends to the client means 71 as approval challenge Challenge703 via the 3rd transmission and reception means 331 (ST7303).

[0170]On the other hand, in the client means 71, it is received by the 1st transmission and reception means 311, the challenge random number 7103 is taken out, and approval challenge Challenge703 is sent to the 1st exclusive OR means 712 (ST7104). When the use approval procedure starting information 7101 is given, the multi stage hash means 317, From said secret memory measure 316, the hash value 3113 is obtained, hash operation H of the number of stages which is equivalent to the difference of the number of times 3112 of effective and the using frequency 7102 at the hash value 3113 is performed, and the multi stage hash value 7104 of a result is sent to the 1st exclusive OR means 712. When the use approval procedure starting information 7101 is given, the 1st exclusive OR means 712, EXCLUSIVE OR operation for every bit is performed between the multi stage hash value 7104 and the challenge random number 7103, The disturbance multi stage hash value 7105 is generated, and it sends to the approval server means 73 as approval challenge answer Response704 via the 1st transmission and reception means 311 (ST7105, ST7106). Since hash operation H cannot calculate this disturbance multi stage hash value 7105 for the sufficiently safe third party who does not know the password PW, the random number R0, and a challenge random number as long as it, on the other hand, has tropism, the length of a result, and random nature, It is shown that it is a valid user which gets to know the password PW by this disturbance multi stage hash value 7105. Since many number of stageses of hash operation H in a multi stage hash value are performed so that it went back in the past and the following multi stage hash value is also incalculable from this multi stage hash value 7104, there is also no necessity for encryption. Generally it is supposed 100 or more times [operation / code] that it is hash operation a high speed, and if it is a suitable number of stages, it can process at high speed than the case where a code is used.

[0171]On the other hand, in the approval server means 73, it is received by the 3rd transmission and reception means 331, the disturbance multi stage hash value 7307 is taken out, and approval challenge answer Response704 is sent to the 2nd exclusive OR means 733 (ST7304). The 2nd exclusive OR means 733 performs EXCLUSIVE OR operation for every bit between the challenge random number 7306 and the disturbance multi stage hash value 7307, obtains the multi stage hash value 7308, and sends it to the 3rd hash means 532 (ST7305). The 3rd hash means 532 performs hash operation to the multi stage hash value 7308, and sends the secondary multi stage hash value 5305 of a result to the approval collation means 337. The approval collation means 337 and the 2nd attestation child addition means 533 operate like the case of drawing 15 and drawing 16, and send the authentication ticket data 5308 to the client means 71 as authentication ticket Ticket501 via the 3rd transmission and reception means 331. However, it is not this limitation, when it remains with the multi stage hash value 5302 and a ticket identifier by reception of authentication ticket rejected note Reject705 and supply of the group 5303 of the number of times of available and a server identifier is deterred (ST7306, ST7307).

[0172]On the other hand, in the client means 71, It is received by the 1st transmission and reception means 311, and authentication ticket Ticket501 is sent to said ticket maintenance management tool 711 as the authentication ticket data 5101, is held (ST7107, ST7108), and is used in a next use approval procedure.

[0173]Since the number of stages of the disturbance multi stage hash value by which the authentication ticket 305 sent to the approval server means 73 is accompanied decreases every [1] for every use approval and it goes from the client means 71 by this, in the approval server means 73, what is necessary is just to perform one step of hash operation, and it can shorten response time. Since a time stamp is updated, it can set to the shortness of the grade which can cover the interval of access to the term of validity, for example, 1 hour, and the user convenience can improve safety, without making it fall. By this method, the client means 71 using the higher authentication ticket 305 of safety, without revealing the password PW to a third party including the approval server means 73 and 74 to n times, Use approval can be obtained in shorter response time, and the authentication ticket is available in common at two or more approval servers, and can decentralize the traffic of check processing.

[0174]Although it had composition which calculates a multi stage hash value in the client means 71 at every use approval procedure in the above explanation, it is good also as composition which carries out precomputation of the multi stage hash value of all the number of stageses at the time of acquisition of an authentication ticket, and is memorized to the secret memory measure 316. In that case, processing time for every use approval procedure of what needs to use the more nearly mass Tampa-proof nature memory device as the secret memory measure 316 can be shortened more.

[0175]Thus, decentralized administration of the use of an authentication ticket can be carried out by constituting an authentication system like this embodiment under the method with which an authentication ticket is updated. Therefore, one management resource can be lessened more.

[0176]

[Effect of the Invention]In this invention, single sign-on type the authentication method and authentication system which cannot need cipher processing in a client side, but can manage the use count of an authentication ticket easily, and can eliminate [1st] double use are obtained so that clearly from the above explanation.

[0177]In a user authentication procedure, cipher processing in a client side is not needed for the 2nd, and also single sign-on type the authentication method and authentication system which can communalize data processing of attestation presentation information and data processing of presentation information are obtained.

[0178]In what generates [3rd] collation information by making into confidential information the random number for attestation which the client means generated. Since the collation information which an authentication ticket includes becomes unrelated to user authentication information, even a possibility that user authentication information will be guessed cannot be found and single sign-on type an authentication method and an authentication system with higher safety are obtained from an authentication ticket.

[0179]By 4th on the other hand performing irreversible arithmetic operation of confidential information by tropism hash operation, even if a client side is a device with low computation capability, single sign-on type the authentication method and authentication system which can perform use approval processing by practical processing time are obtained.

[0180]To the 5th, an approval server means by what updates the collation information of an authentication ticket, etc. Since it is updated whenever an authentication ticket uses it, and especially a time stamp is updated and the term of validity in an effective judging can be set up shorter, Single sign-on type the authentication method and authentication system which possibility of the unauthorized use by a third party can be made smaller, and can shorten the response time of use approval further are obtained.

[0181]In what established the authentication ticket management tool which manages [6th] the use count of an authentication ticket. In the system by which an authentication ticket is not updated, since it becomes possible to use an authentication ticket in common to two or more approval servers, single sign-on type an authentication method and an authentication system with higher convenience are obtained.

[0182]To the 7th, an authentication server means and an approval server means by what memorizes the issuance history of an authentication ticket. In the system by

which an authentication ticket is updated, since the decentralized administration of the use of an authentication ticket can be carried out, single sign-on type the authentication method and authentication system which can lessen one management resource more are obtained.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The key map showing the outline of the authentication system in a 1st embodiment of this invention,

[Drawing 2]The key map showing the outline of the authentication system in a 2nd embodiment of this invention,

[Drawing 3]The key map showing the outline of the authentication system in a 3rd embodiment of this invention,

[Drawing 4]The protocol sequence diagram of the authentication system in a 4th embodiment of this invention,

[Drawing 5]The functional block diagram of the authentication system in a 4th embodiment of this invention,

[Drawing 6]The flow chart showing operation of the authentication system in a 4th embodiment of this invention,

[Drawing 7]The detailed functional block diagram of the attestation child addition means at the time of using a message authorization code in the authentication system in a 4th embodiment of this invention,

[Drawing 8]The detailed functional block diagram of the attestation child verifying means at the time of using a message authorization code in the authentication system in a 4th embodiment of this invention,

[Drawing 9]The detailed functional block diagram of the attestation child addition means at the time of using a digital signature in the authentication system in a 4th embodiment of this invention,

[Drawing 10]The detailed functional block diagram of the attestation child verifying means at the time of using a digital signature in the authentication system in a 4th embodiment of this invention,

[Drawing 11]The protocol sequence diagram of the authentication system in a 5th embodiment of this invention,

[Drawing 12]The functional block diagram of the authentication system in a 5th embodiment of this invention,

[Drawing 13]The flow chart showing operation of the authentication system in a 5th embodiment of this invention,

[Drawing 14]The protocol sequence diagram of the authentication system in a 6th embodiment of this invention,
[Drawing 15]The functional block diagram of the authentication system in a 6th embodiment of this invention,
[Drawing 16]The flow chart showing operation of the authentication system in a 6th embodiment of this invention,
[Drawing 17]The protocol sequence diagram of the authentication system in a 7th embodiment of this invention,
[Drawing 18]The functional block diagram of the authentication system in a 7th embodiment of this invention,
[Drawing 19]The flow chart showing operation of the authentication system in a 7th embodiment of this invention,
[Drawing 20]The protocol sequence diagram of the authentication system in an 8th embodiment of this invention,
[Drawing 21]The functional block diagram of the authentication system in an 8th embodiment of this invention,
[Drawing 22]The flow chart showing operation of the authentication system in an 8th embodiment of this invention,
[Drawing 23]The key map showing the outline of the conventional authentication method,
[Drawing 24]The protocol sequence diagram of the conventional authentication method,
[Drawing 25]The functional block diagram of the conventional authentication method,
[Drawing 26]It is a flow chart showing operation of the conventional authentication method.
[Description of Notations]
1, 11, 21, 31, 41, 51, 61, 71, 81 client means
2, 12, 22, 32, 42, 62, 72, 82 authentication server means
3, 33, 53, 63, 73, and 83 Approval server means
4, 14, and 24 Confidential information
5, 7, 803, 805 authentication tickets
6 and 804 Presentation information
8 and 806 Notice of approval
13, 23, and 801 Attestation presentation information
64 Authentication ticket management tool
74 The 2nd approval server means
311 The 1st transmission and reception means
312 and 811 Input means
313 Hash means
314 Ticket holding mechanism

316 A secret memory measure
317 Multi stage hash means
321 The 2nd transmission and reception means
322 attestation -- a time check -- a means
323 Authentication information storage means
324 Random number generating means
325 The 2nd multi stage hash means
326 Attestation collation means
327 Ticket identifier creating means
328 Attestation child addition means
328A self-identifier storage means
328B data connecting mechanism
328C connection data hash means
328D server common key memory measure
328E common key system cryptographer stage
328F attestation child connecting mechanism
328G self-secret key memory measure
328H public key system cryptographer stage
331 The 3rd transmission and reception means
332 approval -- a time check -- a means
333 Attestation child verifying means
333A attestation child separating mechanism
the [333B] -- the connection data hash means of two
the [333C] -- the server common key memory measure of two
the [333D] -- the common key system cryptographer stage of two
333E data separation means
333F publisher identifier collation means
333G comparison means
333H server public key accumulation means
333J public key system decoding means
334 and 832 Ticket effective judging means
335 and 531 Ticket use management tool
336 The 3rd multi stage hash means
337 Approval collation means
411 The random number generating means for attestation
412, 612, and 712 The 1st exclusive OR means
421 The 2nd hash means
422 The 2nd exclusive OR means
423 The 2nd multi stage hash means
511 Ticket holding mechanism

532 The 3rd hash means
533 The 2nd attestation child addition means
611 and 711 Ticket maintenance management tool
621 Ticket registration instruction means
631 Ticket update indication means
632 The 2nd random number generating means
633 and 733 The 2nd exclusive OR means
721 Ticket issue management tool
731 Renewal management tool of a ticket
732 The 2nd random number generating means
812 Session key decoding means
813 proof -- a time check -- a means
814 Certification information cryptographer stage
821 Session key creating means
822 Session key cryptographer stage
823 Ticket cryptographer stage
831 Ticket decoding means
833 Certification information decoding means
834 Certification information effective judging means
835 Approval collation means

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－222360
（P2000－222360A）
(43)公開日　平成12年８月11日(2000.8.11)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｂ	５Ｂ０１７
	12/14	３２０	12/14	３２０Ｃ	５Ｂ０５８
	13/00	３５４	13/00	３５４Ｚ	５Ｂ０８５
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ 17/00	Ｔ	５Ｂ０８９
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ 9/00	６７５Ａ	５Ｊ１０４

審査請求　未請求　請求項の数29　ＯＬ　（全 48 頁）

(21)出願番号　特願平11－24446

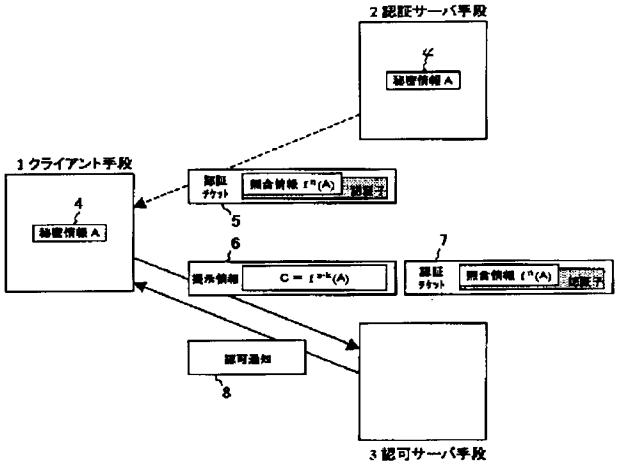
(22)出願日　平成11年２月１日(1999.2.1)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　柴田　顕男
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　高山　久
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100099254
弁理士　役　昌明　（外３名）

最終頁に続く

(54)【発明の名称】　認証方法、認証システム及び認証処理プログラム記録媒体

(57)【要約】
【課題】　１回のユーザ認証で複数回のアクセスを許可するシングルサインオン型認証において、少ない計算量で正当なアクセスを判別し、不正なアクセスを排除する。
【解決手段】　クライアント手段１と認証サーバ手段２とで秘密情報４を共有する。認証サーバ手段２は秘密情報４に不可逆演算ｆをｎ回行なった照合情報を含んだ認証チケット５を発行する。クライアント手段１はこの認証チケットとともに、秘密情報４に不可逆演算ｆをｎ－ｋ回行なった提示情報を認可サーバ手段３に示す。認可サーバ手段はこの提示情報に不可逆演算ｆをｋ回行なって、照合情報と一致するかをチェックする。ｋを１からｎまで増加させることにより、過去の提示情報から次の提示情報を計算されることなく、最大ｎ回のアクセスに認証チケット５が使用できる。



【特許請求の範囲】

【請求項１】　認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムにおいて、
有効回数がｎ（ｎは正整数）である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて前記クライアント手段に提示情報を要求し前記認証チケットと照合して利用を認可する認可サーバ手段とを具備し、前記認証チケットは、チケット識別子と照合情報と有効回数とを含み、且つ、認証子が付与されており、前記照合情報は、前記認証サーバ手段と前記クライアント手段とが共有する秘密情報に所定の不可逆演算をｎ回施したものであり、前記認証チケットの使用回数がｋ（ｋはｎ以下の正整数）であるときの前記提示情報は、前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施したものであることを特徴とする認証システム。

【請求項２】　前記認証サーバ手段が、ユーザ認証情報を管理し、前記クライアント手段との間でユーザ認証手順を実行して前記認証チケットを発行することを特徴とする請求項１に記載の認証システム。

【請求項３】　前記認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示して前記クライアント手段に認証提示情報を要求し、前記秘密情報は、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を１回以上施したものであり、前記認証提示情報は、前記秘密情報に前記所定の不可逆演算をｎ回施したものであることを特徴とする請求項２に記載の認証システム。

【請求項４】　前記認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求し、前記認証提示情報が、前記ユーザ認証情報及び前記乱数との連結に前記所定の不可逆演算を１回以上施したものと前記クライアント手段が生成した認証用乱数との排他的論理和演算結果であり、前記秘密情報が、前記認証提示情報から逆算される前記認証用乱数であることを特徴とする請求項２に記載の認証システム。

【請求項５】　前記ユーザ認証情報が、ユーザにより入力されるパスワードであることを特徴とする請求項２から４のいずれかに記載の認証システム。

【請求項６】　前記ユーザ認証情報が、秘密裏に保持された共通鍵方式暗号鍵であることを特徴とする請求項２から４のいずれかに記載の認証システム。

【請求項７】　前記認証子が、メッセージ認証コードであることを特徴とする請求項１から６のいずれかに記載の認証システム。

【請求項８】　前記認証子が、デジタル署名であることを特徴とする請求項１から６のいずれかに記載の認証システム。

【請求項９】　前記所定の不可逆演算が、一方向性ハッシュ演算であることを特徴とする請求項１から８のいずれかに記載の認証システム。

【請求項１０】　前記認証チケットが、サーバ識別子を含むことを特徴とする請求項１から９のいずれかに記載の認証システム。

【請求項１１】　前記認証チケットが、発行日時を含むことを特徴とする請求項１から１０のいずれかに記載の認証システム。

【請求項１２】　前記認証チケットが、発行者識別子を含み、前記認可サーバ手段が、利用認可するとともに前記認証チケットの照合情報と有効回数と発行日時と発行者識別子と認証子とを更新し、前記照合情報が、前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施したものに更新され、前記有効回数がｎ－ｋに更新されることを特徴とする請求項１１に記載の認証システム。

【請求項１３】　前記認可サーバ手段が、前記認証チケットの使用回数を管理しており、これを示して提示情報を要求することを特徴とする請求項１から１２のいずれかに記載の認証システム。

【請求項１４】　前記クライアント手段が、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めることを特徴とする請求項１から１２のいずれかに記載の認証システム。

【請求項１５】　複数の前記認可サーバ手段と、前記認証チケットの使用回数を管理する認証チケット管理手段とを備えており、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認証サーバ手段は、前記認証チケットを発行するとともに前記認証チケット管理手段に前記認証チケットの発行登録を指示し、前記認可サーバ手段は、前記認証チケットの提示を受けて前記認証チケット管理手段に前記認証チケットの履歴更新を指示し、前記認証チケット管理手段より拒絶通知を受けた場合には利用認可しないことを特徴とする請求項１から１１のいずれかに記載の認証システム。

【請求項１６】　前記認可サーバ手段を複数備え、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認証サーバ手段は、前記認証チケットを発行するとともに発行履歴を記憶し、前記認可サーバ手段は、前記認証チケットを更新するとともに更新履歴を記憶し、前記認証チケットの提示を受けて前記認証チケットの発行者識別子が示す前記認証サーバ手段または前記認可サーバ手段に前記認証チケットの履歴を照会し、前記認証サーバ手段または前記認可サーバ手段より拒絶通知を受けた場合には利用認可しない

ことを特徴とする請求項１２に記載の認証システム。

【請求項１７】　前記認可サーバ手段は、利用認可手順において乱数を生成し、これを示して提示情報を要求するものであり、前記認証チケットの使用回数がｋであるときの前記提示情報は前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施したものと前記乱数との排他的論理和演算結果であることを特徴とする請求項１４から１６のいずれかに記載の認証システム。

【請求項１８】　認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムにおいて、

前記クライアント手段が、ユーザ識別子とユーザ認証情報とサーバ識別子と認証チケットの有効回数の入力を得る入力手段と、前記認証サーバ手段より認証チケットを得て保持し、前記認可サーバ手段に提示するチケット保持手段と、前記チケット保持手段より認証チケットの有無情報を得て処理を選択する処理選択手段と、前記入力手段よりユーザ認証情報を得るとともに前記認証サーバ手段より乱数を得て、これらの連結にハッシュ演算を施すハッシュ手段と、前記ハッシュ手段より得たハッシュ値を秘密裏に記憶する機密記憶手段と、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においては前記入力手段より有効回数ｎ（ｎは正整数）を得て、ｎ段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記認可サーバ手段より利用回数ｋ（ｋはｎ以下の正整数）を得て、ｎ－ｋ段のハッシュ演算を施して得た多段ハッシュ値を前記認可サーバ手段に送る多段ハッシュ手段とを具備し、

前記認証サーバ手段が、ユーザ認証情報が蓄積された認証情報蓄積手段と、乱数を生成して前記クライアント手段に送る乱数生成手段と、前記認証情報蓄積手段より得たユーザ認証情報と前記乱数生成手段で生成した乱数との連結にｎ＋１段のハッシュ演算を行なう第２の多段ハッシュ手段と、前記クライアント手段より得た多段ハッシュ値を前記第２の多段ハッシュ手段で得た多段ハッシュ値と照合する認証照合手段と、有効なチケット識別子を生成するチケット識別子生成手段と、時刻を計時し時刻情報を出力する認証計時手段と、前記チケット識別子生成手段より得たチケット識別子、前記認証照合手段より得た多段ハッシュ値、前記クライアント手段より得たサーバ識別子及び有効回数、前記認証計時手段より得た時刻情報に基づくタイムスタンプ、並びに認証サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送る認証子付加手段とを具備し、

前記認可サーバ手段が、前記クライアント手段より得た認証チケットの認証子を検証する認証子検証手段と、時刻を計時し時刻情報を出力する認可計時手段と、サーバ識別子の妥当性及びタイムスタンプと前記認可計時手段より得た時刻情報との差の有効性をチェックするチケット有効判定手段と、認証チケットのチケット識別子と利用回数と残り利用可能回数とを管理するチケット利用管理手段と、前記チケット利用管理手段より利用回数ｋを得て、前記クライアント手段より得た多段ハッシュ値にｋ段のハッシュ演算を施して得た二次多段ハッシュ値を出力する第３の多段ハッシュ手段と、前記チケット利用管理手段より得た多段ハッシュ値と前記第３の多段ハッシュ手段より得た二次多段ハッシュ値とを照合する認可照合手段とを具備することを特徴とする認証システム。

【請求項１９】　前記認証子付加手段が、サーバ間で共有する共通鍵方式暗号鍵を記憶するサーバ共通鍵記憶手段と、自識別子を記憶する自識別子記憶手段と、チケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と前記自識別子記憶手段より得た発行者識別子とを連結するデータ連結手段と、前記データ連結手段より得た連結データにハッシュ演算を施す連結データハッシュ手段と、前記サーバ共通鍵記憶手段より得た共通鍵方式暗号鍵を用いて前記連結データハッシュ手段より得たハッシュ値を暗号化して認証子とする共通鍵方式暗号手段と、前記データ連結手段より得た連結データと前記共通鍵方式暗号手段より得た認証子とを連結する認証子連結手段とを具備し、

前記認証子検証手段が、サーバ間で共有する共通鍵方式暗号鍵を記憶する第２のサーバ共通鍵記憶手段と、認証チケットを連結データと認証子とに分離する認証子分離手段と、前記認証子分離手段より得た連結データをチケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と発行者識別子とに分離するデータ分離手段と、前記認証子分離手段より得た連結データにハッシュ演算を施す第２の連結データハッシュ手段と、前記第２のサーバ共通鍵記憶手段より得た共通鍵方式暗号鍵を用いて前記第２の連結データハッシュ手段より得たハッシュ値を暗号化して比較用認証子とする第２の共通鍵方式暗号手段と、前記データ分離手段より得た発行者識別子が有効なサーバ識別子であることをチェックする発行者識別子照合手段と、前記発行者識別子照合手段より得た照合結果が有効を示す場合に前記認証子分離手段より得た認証子と前記第２の共通鍵方式暗号手段より得た比較用認証子とを比較して結果を出力する比較手段とを具備することを特徴とする請求項１８に記載の認証システム。

【請求項２０】　前記認証子付加手段が、認証サーバの公開鍵方式暗号秘密鍵を秘密裏に記憶する自秘密鍵記憶手段と、自識別子を記憶する自識別子記憶手段と、チケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と前記自識別子記憶手段より得た発行者識別子とを連結するデータ連結手段と、前記データ連

結手段より得た連結データにハッシュ演算を施す連結データハッシュ手段と、前記自秘密鍵記憶手段より得た公開鍵方式暗号秘密鍵を用いて前記連結データハッシュ手段より得たハッシュ値を暗号化して認証子とする公開鍵方式暗号手段と、前記データ連結手段より得た連結データと前記公開鍵方式暗号手段より得た認証子とを連結する認証子連結手段とを具備し、
前記認証子検証手段が、認証チケットを連結データと認証子とに分離する認証子分離手段と、前記認証子分離手段より得た連結データをチケット識別子と多段ハッシュ値と有効回数とタイムスタンプとサーバ識別子と発行者識別子とに分離し出力するデータ分離手段と、前記認証子分離手段より得た連結データにハッシュ演算を施す第２の連結データハッシュ手段と、有効なサーバの公開鍵方式暗号公開鍵が蓄積され前記データ分離手段より得た発行者識別子に対応する公開鍵方式暗号公開鍵を出力するサーバ公開鍵蓄積手段と、前記サーバ公開鍵蓄積手段より得た公開鍵方式暗号公開鍵を用いて前記認証子分離手段より得た認証子を復号し比較用ハッシュ値とする公開鍵方式復号手段と、前記連結データハッシュ手段より得たハッシュ値と前記公開鍵方式復号手段より得た比較用ハッシュ値とを比較して結果を出力する比較手段とを具備することを特徴とする請求項１８に記載の認証システム。

【請求項２１】　前記クライアント手段が、認証乱数生成手段と第１の排他的論理和手段とを具備し、前記認証用乱数生成手段は、ユーザ認証手順において認証用乱数を生成し、前記第１の排他的論理和手段は、ユーザ認証手順において前記認証用乱数生成手段より得た認証用乱数と前記ハッシュ手段より得たハッシュ値との排他的論理和演算を行なって得た撹乱ハッシュ値を前記認証サーバ手段に送り、前記機密記憶手段は、前記認証用乱数生成手段より得た認証用乱数を秘密裏に記憶し、前記多段ハッシュ手段は、前記機密記憶手段より認証用乱数を取り出して、利用認可手順において前記認可サーバ手段より利用回数ｋを得て、ｎ－ｋ段のハッシュ演算を施して得た多段ハッシュ値を前記認可サーバ手段に送り、
前記認証サーバ手段が、前記認証照合手段に代わり第２のハッシュ手段及び第２の排他的論理和手段を具備し、前記第２のハッシュ手段は、前記認証情報蓄積手段より得たユーザ認証情報と前記乱数生成手段で生成した乱数との連結にハッシュ演算を施し、前記第２の排他的論理和手段は、前記第２のハッシュ手段より得たハッシュ値と前記クライアント手段より得た撹乱ハッシュ値との排他的論理和演算を行なって認証用乱数を取得し、前記第２の多段ハッシュ手段は、前記第２の排他的論理和手段より得た認証用乱数にｎ段のハッシュ演算を行ない、前記認証子付加手段は、前記チケット識別子生成手段より得たチケット識別子、前記第２の多段ハッシュ手段より得た多段ハッシュ値、前記クライアント手段より得たサーバ識別子及び有効回数、前記認証計時手段より得た時刻情報に基づくタイムスタンプ、並びに認証サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項１８から２０のいずれかに記載の認証システム。

【請求項２２】　前記認可サーバ手段が、前記第３の多段ハッシュ手段に代わり第３のハッシュ手段及び第２の認証子付加手段を具備し、前記第３のハッシュ手段は、前記クライアント手段より得た多段ハッシュ値にハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記認可照合手段は、前記チケット利用管理手段より得た多段ハッシュ値と前記第３のハッシュ手段より得た二次多段ハッシュ値とを照合し、前記第２の認証子付加手段は、前記チケット利用管理手段より得たチケット識別子、サーバ識別子及び残り利用回数、前記クライアント手段より得た多段ハッシュ値、前記認可計時手段より得た時刻情報に基づくタイムスタンプ、並びに認可サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項１８から２１のいずれかに記載の認証システム。

【請求項２３】　１つ以上の認可サーバ手段と、認証チケットの発行及び利用状況を管理する認証チケット管理手段とを具備し、前記認証チケット管理手段が、前記認証サーバ手段より得た認証チケット発行登録指示をもとにチケット識別子と有効回数と残り利用回数との組を管理して、前記認可サーバ手段より得た認証チケット履歴更新指示との整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送り、
前記認証サーバ手段が、チケット登録指示手段を具備し、前記チケット登録指示手段は、前記チケット識別子生成手段より得たチケット識別子と前記クライアント手段より得たサーバ識別子及び有効回数とから認証チケット発行登録指示を生成して前記認証チケット管理手段に送り、
前記クライアント手段が、前記チケット保持手段に代わるチケット保持管理手段と、第１の排他的論理和手段とを具備し、前記チケット保持管理手段は、前記認証サーバ手段より認証チケットを得て保持するとともに利用回数を管理して、前記認可サーバ手段にそれらを提示し、前記多段ハッシュ手段は、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においてはｎ段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記チケット保持管理手段より得た利用回数ｋを得て、ｎ－ｋ段のハッシュ演算を施して得た多段ハッシュ値を前記第１の排他的論理和手段に送り、前記第１の排他的論理和手段は、前記多段ハッシュ手段より得た多段ハッシュ値と前記認可サーバ手段より得た乱数との排他的論理和演算を行な

って結果の撹乱多段ハッシュ値を前記認可サーバ手段に送り、
前記認可サーバ手段が、チケット利用管理手段に代わるチケット更新指示手段と、第２の乱数生成手段と、第２の排他的論理和手段とを具備し、前記チケット更新指示手段は、前記チケット有効判定手段より得た判定結果が有効を示す場合に前記認証子検証手段より得たチケット識別子及びサーバ識別子と前記クライアント手段より得た利用回数とから認証チケット履歴更新指示を生成して前記認証チケット管理手段に送り、前記認証チケット管理手段より認証チケット拒絶通知が返されなかった場合に前記クライアント手段より得た利用回数ｋと前記認証子検証手段より得た多段ハッシュ値とを出力し、前記第２の乱数生成手段は、乱数を生成して前記クライアント手段及び前記第２の排他的論理和手段に送り、前記第２の排他的論理和手段は、前記第２の乱数生成手段より得た乱数と前記クライアント手段より得た撹乱多段ハッシュ値との排他的論理和演算を行なって多段ハッシュ値を取得し、前記第３の多段ハッシュ手段は、前記第２の排他的論理和手段より得た多段ハッシュ値にｋ段のハッシュ演算を施して得た二次多段ハッシュ値を出力し、
前記認証チケット管理手段は、前記認証サーバ手段より得た認証チケット発行登録指示をもとにチケット識別子と有効回数と残り利用回数との組を管理し、前記認可サーバ手段より得た認証チケット履歴更新指示との整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送ることを特徴とする請求項１８から２１のいずれかに記載の認証システム。
【請求項２４】　認可サーバ手段を１つ以上具備し、前記認証サーバ手段が、チケット発行管理手段を具備し、前記チケット発行管理手段は、前記チケット識別子生成手段より得たチケット識別子と前記クライアント手段より得たサーバ識別子及び有効回数とを管理し、前記認可サーバ手段より得たチケット利用照会をもとにチケット識別子を検索して利用回数の整合性をチェックし、不整合の場合には前記認可サーバ手段に認証チケット拒絶通知を送り、
前記クライアント手段が、前記チケット保持手段に代わるチケット保持管理手段と、第１の排他的論理和手段とを具備し、前記チケット保持管理手段は、前記認証サーバ手段より認証チケットを得て保持するとともに利用回数を管理して、前記認可サーバ手段にそれらを提示し、前記多段ハッシュ手段は、前記機密記憶手段よりハッシュ値を取り出して、ユーザ認証手順においてはｎ段のハッシュ演算を施して得た多段ハッシュ値を前記認証サーバ手段に送り、利用認可手順においては前記チケット保持管理手段より得た利用回数ｋを得て、ｎ－ｋ段のハッシュ演算を施して得た多段ハッシュ値を前記第１の排他的論理和手段に送り、前記第１の排他的論理和手段は、前記多段ハッシュ手段より得た多段ハッシュ値と前記認可サーバ手段より得た乱数との排他的論理和演算を行なって結果の撹乱多段ハッシュ値を前記認可サーバ手段に送り、
前記認可サーバ手段が、前記チケット利用管理手段に代わるチケット更新管理手段と、第２の乱数生成手段及び第２の排他的論理和手段とを具備し、前記チケット更新管理手段は、前記チケット有効判定手段より得た判定結果が有効を示す場合に前記認証子検証手段より得たチケット識別子及びサーバ識別子と前記クライアント手段より得た利用回数とからチケット利用照会を生成し、発行者識別子が示す前記認証サーバ手段または第２の認可サーバ手段に対して送り、前記認証サーバ手段または前記第２の認可サーバ手段より認証チケット拒絶通知が返されなかった場合に、前記クライアント手段より得た利用回数と前記認証子検証手段より得た多段ハッシュ値とを出力するとともに、チケット識別子、サーバ識別子及び残り利用回数を管理して、前記第２の認可サーバ手段よりチケット利用照会を受けた場合に利用回数の整合性をチェックし、不整合の場合には前記第２の認可サーバ手段に認証チケット拒絶通知を送り、前記第２の乱数生成手段は、乱数を生成して前記クライアント手段及び前記第２の排他的論理和手段に送り、前記第２の排他的論理和手段は、前記第２の乱数生成手段より得た乱数と前記クライアント手段より得た撹乱多段ハッシュ値との排他的論理和演算を行なって多段ハッシュ値を取得し、前記第２のハッシュ手段は、前記第２の排他的論理和手段より得た多段ハッシュ値にハッシュ演算を施して得た二次多段ハッシュ値を出力し、前記第２の認証子付加手段は、前記チケット管理手段より得たチケット識別子、サーバ識別子及び残り利用回数、前記第２の排他的論理和手段より得た多段ハッシュ値、前記認可計時手段より得た時刻情報に基づくタイムスタンプ、並びに認可サーバ手段を示す発行者識別子の連結に認証子を付加し、認証チケットとして前記クライアント手段に送ることを特徴とする請求項２２に記載の認証システム。
【請求項２５】　認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムの認証方法において、
認証サーバ手段からクライアント手段に、認証サーバ手段とクライアント手段とが共有する秘密情報に所定の不可逆演算をｎ（ｎは正整数）回施した照合情報を含む、有効回数がｎである認証チケットを発行し、クライアント手段は、前記認証チケットを認可サーバ手段に示して利用認可を求め、認可サーバ手段の提示情報の要求に対して、クライアント手段は、前記認証チケットの使用回数がｋ（ｋはｎ以下の正整数）であるとき、前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施した演算結果を

前記提示情報として提示し、認可サーバ手段は、前記提示情報に前記所定の不可逆演算をｋ回施し、その演算結果と前記照合情報との一致を識別することを特徴とする認証方法。

【請求項２６】　認証チケットを発行する認証サーバ手段と、認証チケットの利用を認可する認可サーバ手段と、前記認証サーバ手段に認証チケットを要求し、前記認可サーバ手段に認証チケットの利用認可を要求するクライアント手段とを備える認証システムの認証方法において、

認証サーバ手段からクライアント手段に、認証サーバ手段とクライアント手段とが共有する秘密情報に所定の不可逆演算をｎ（ｎは正整数）回施した照合情報を含む、有効回数がｎである認証チケットを発行し、クライアント手段は、前記認証チケットを認可サーバ手段に示して利用認可を求め、認可サーバ手段の提示情報の要求に対して、クライアント手段は、前記認証チケットの使用回数がｋ（ｋはｎ以下の正整数）であるとき、前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施した演算結果を前記提示情報として提示し、認可サーバ手段は、前記提示情報に前記所定の不可逆演算を１回施し、その演算結果と前記照合情報との一致を識別するとともに、前記認証チケットに含まれる照合情報を前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施した演算結果に更新することを特徴とする認証方法。

【請求項２７】　前記認証サーバ手段が、認証チケットを要求するクライアント手段に乱数を示して認証提示情報を要求し、クライアント手段は、ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算をｎ＋１回施した演算結果を前記認証提示情報として提示し、認証サーバ手段は、保持しているユーザ認証情報と前記乱数との連結に前記所定の不可逆演算をｎ＋１回施して、その演算結果と前記認証提示情報との一致を確認すると、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を１回施した演算結果を前記秘密情報として、これに所定の不可逆演算をｎ（ｎは正整数）回施した前記照合情報を含む認証チケットを発行することを特徴とする請求項２５または２６に記載の認証方法。

【請求項２８】　前記認証サーバ手段が、認証チケットを要求するクライアント手段に乱数を示して認証提示情報を要求し、クライアント手段は、ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を１回以上施したものとクライアント手段が生成した認証用乱数との排他的論理和演算結果を前記認証提示情報として提示し、認証サーバ手段は、保持しているユーザ認証情報と前記乱数とを用いて前記認証提示情報から前記認証用乱数を逆算し、前記認証用乱数を前記秘密情報として、これに所定の不可逆演算をｎ（ｎは正整数）回施した前記照合情報を含む認証チケットを発行することを特徴とする請求項２５または２６に記載の認証方法。

【請求項２９】　請求項１から２４のいずれかに記載の認証システムで実行される認証方法または請求項２５から２８のいずれかに記載の認証方法の処理プログラムを、電子計算機が読取り可能な形式で記録した、認証処理プログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、クライアント装置がサーバ装置にアクセスすることの妥当性を判断する１回の処理をもって複数回のアクセスを許可する、シングルサインオン型の認証方法及び認証システムに関し、特に、クライアント装置での暗号処理を不要にし、計算処理能力が低い装置でも処理できるようにしたものである。

【０００２】

【従来の技術】近年、デジタル通信技術の発達にともない、ネットワークを介して接続されたサーバ装置及びクライアント装置から構成されるサーバ・クライアント型システムが一般的なものとなって来た。そのようなサーバ・クライアント型システムにおいては、クライアント装置及びそのユーザがサーバ装置にアクセスする正当な権限を有することを確認し、不正なアクセスが行なわれないようにすることが重要である。このアクセス権限を確認する認証方法としては、パスワード入力によるものが良く知られるが、アクセスする度にパスワード入力を求める方法は安全である反面ユーザにとっては不便であるため、利便性を向上させたシングルサインオン型の認証方法が利用されるようになって来た。このようなシングルサインオン型の認証方法としては、例えば、Ｋｅｒｂｅｒｏｓ認証システムで用いられるＴＴＰ（Trusted Third-party Protocol）が一般に知られている。

【０００３】以下、従来のシングルサインオン型の認証方法について図面を参照しながら説明する。図２３は従来のシングルサインオン型の認証方法の概要を示す概念図であり、図２４はプロトコルを示すプロトコルシーケンス図である。図２３及び図２４において、81はユーザインタフェースを持つクライアント手段、82はユーザ認証を行なう認証サーバ手段、83はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【０００４】クライアント手段81と認証サーバ手段82とのユーザ認証手順においては、ユーザインタフェースを介して入力されたユーザ識別子ＵＩＤとサーバ識別子ＳＩＤとを認証提示情報としてともなった認証要求Authenticate Request801をクライアント手段81が認証サーバ手段82に送り、これに対し認証サーバ手段82がパスワードＰＷを鍵として暗号化されたセッション鍵ＳＫをともなった認証応答Authorize Request802を認証チケットTicket803とともに送り返す。

【０００５】さらに、クライアント手段81と認可サーバ手段83との利用認可手順においては、クライアント手段

81がセッション鍵ＳＫで暗号化されたユーザ識別子ＵＩＤとタイムスタンプＴＳｋとを提示情報としてともなった認可要求Authorize Request804を認証チケットTicket805とともに認可サーバ手段83に送り、これに対し認可サーバ手段83は認証要求Authorize Request804における提示情報と認証チケットTicket805とを検証して、正当と認めれば認可通知Result806を送り返すものである。

【０００６】以上のようなプロトコルシーケンスを持つ従来のシングルサインオン型の認証方法において、以下その構成について図２５を参照しながら説明する。図２５は、従来のシングルサインオン型の認証方法の構成を示す機能ブロック図である。図２５においても、81はユーザインタフェースを持つクライアント手段、82はユーザ認証を行なう認証サーバ手段、83はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【０００７】クライアント手段81は、データの送受信を行なう第１の送受信手段311と、ユーザからの入力を得る入力手段811と、受信したセッション鍵を復号するセッション鍵復号手段812と、受信した認証チケットを保持するチケット保持手段314と、認証チケットの保持状態に応じて処理を選択する処理選択手段315と、復号したセッション鍵を秘密裏に記憶する機密記憶手段316と、時刻を計時する証明計時手段813と、セッション鍵を用いて認証済み証明情報を暗号化する証明情報暗号手段814とから構成される。

【０００８】また、認証サーバ手段82は、データの送受信を行なう第２の送受信手段321と、時刻を計時する認証計時手段322と、パスワード等のユーザ認証情報が蓄積された認証情報蓄積手段323と、ユーザ認証処理毎に暗号鍵を生成するセッション鍵生成手段821と、パスワードを用いてセッション鍵を暗号化するセッション鍵暗号手段822と、セッション鍵を用いて認証チケットを暗号化するチケット暗号手段823とから構成される。

【０００９】また、認可サーバ手段83は、データの送受信を行なう第３の送受信手段331と、時刻を計時する認可計時手段332と、認証チケットを復号するチケット復号手段831と、認証チケットの有効性判定を行なうチケット有効判定手段832と、認証済み証明情報を復号化する証明情報復号手段833と、認証済み証明情報の有効性判定を行なう証明情報有効判定手段834と、認証チケットの内容と認証済み証明情報の内容とを比較照合する認可照合手段835とから構成される。

【００１０】以上のように構成された従来のシングルサインオン型の認証方法において、以下その動作について図２６を参照しながら説明する。まず、クライアント手段81において、ユーザ自身を示すユーザ識別子ＵＩＤと認証サーバ手段82にあらかじめ登録されたユーザ認証用のパスワードＰＷと利用認可を得る対象のサーバ識別子ＳＩＤとがユーザ入力800として入力手段811に入力される（ＳＴ３１０１、ＳＴ８１０１）。入力手段811は、ユーザ入力800を一時保持するとともにサーバ識別子3101を取出してチケット保持手段314に送る。チケット保持手段314は、サーバ識別子3101に対応する認証チケットデータを検索して（ＳＴ３１０２）、検索結果通知3102を処理選択手段315に送る。処理選択手段315は、検索結果通知3102が無しを示す場合には、ユーザ認証処理起動通知8101を前記入力手段811に送り、有りを示す場合には、利用認可手順起動通知8102を前記チケット保持手段314、機密記憶手段316及び証明情報暗号手段814に送る（ＳＴ３１０３）。

【００１１】前記入力手段811は、ユーザ認証起動通知8101が与えられると、一時保持したユーザ入力800から取出した、ユーザ識別子とサーバ識別子との組8103を第１の送受信手段311を介して認証要求Authenticate Request801として認証サーバ手段82に送り（ＳＴ８１０２）、ユーザ識別子8104を証明情報暗号手段814に送り、パスワード8105をセッション鍵復号手段812に送る。

【００１２】認証サーバ手段82においては、認証要求Authenticate Request801は第２の送受信手段321で受信され、取出されたユーザ識別子8201が認証情報蓄積手段323及びチケット暗号手段823に送られ、サーバ識別子8202がチケット暗号手段823に送られる（ＳＴ８２０１）。認証情報蓄積手段323は、ユーザ識別子8201に対応するパスワードを検索して（ＳＴ８２０２）、有りの場合にはパスワード8203をセッション鍵暗号手段822に送り、検索結果通知8204をセッション鍵生成手段821及びセッション鍵暗号手段822に送る（ＳＴ８２０３）。セッション鍵生成手段821は、検索結果通知8204が有りを示す場合に、新たにランダムなセッション鍵8205を生成してセッション鍵暗号手段822及びチケット暗号手段823に送る（ＳＴ８２０４）。セッション鍵暗号手段822は、検索結果通知8204が有りを示す場合に、セッション鍵8205をパスワード8203を用いて暗号化した暗号化セッション鍵8206を生成し（ＳＴ８２０５）、これを第２の送受信手段321を介して認証応答Authenticate Response802としてクライアント手段81に送る（ＳＴ８２０７）。認証計時手段322は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3212をチケット暗号手段823に供給している。チケット暗号手段823は、内部に保持しサーバ識別子8202に対応したサーバ共通鍵を用いて、ユーザ識別子8201とサーバ識別子8202とタイムスタンプ3212とセッション鍵8205とを暗号化した認証チケットデータ8207を生成し（ＳＴ８２０２、ＳＴ８２０６）、これを第２の送受信手段321を介して認証チケットTicket803としてクライアント手段81に送る（ＳＴ８２０７）。

【００１３】クライアント手段81においては、認証応答Authenticate Response802は第１の送受信手段311を介して暗号化セッション鍵8106としてセッション鍵復号手段812に送られ、認証チケットTicket803は第１の送受信手段311を介して認証チケットデータ8108として前記チ

ケット保持手段314に送られる（ＳＴ８１０３）。前記チケット保持手段314は認証チケットデータ8108をサーバ識別子3101と対応づけて保持する（ＳＴ３１１２）。セッション鍵復号手段812は、暗号化セッション鍵8106をパスワード8105を用いて復号化する（ＳＴ８１０４）。従って、正しいパスワードが入力された場合にのみ正しいセッション鍵を得ることができる。セッション鍵復号手段812で得られたセッション鍵8107は機密記憶手段316に送られ記憶される。

【００１４】機密記憶手段316は、セッション鍵8107を秘密裏に記憶して所定のアクセスのみ許容するもので（ＳＴ８１０５）、利用認可手順起動通知8102が与えられた場合に、記憶したセッション鍵8109を証明情報暗号手段814に送る。証明計時手段813は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ8110を証明情報暗号手段814に供給している。証明情報暗号手段814は、利用認可手順起動通知8102が与えられると、ユーザ識別子8104とタイムスタンプ8110とをセッション鍵8109を用いて暗号化した認証済み証明情報8111を生成し（ＳＴ８１０６）、これを第１の送受信手段311を介して認可要求Authorize Request804として認可サーバ手段83に送る（ＳＴ８１０７）。前記チケット保持手段314は、利用認可手順起動通知8102が与えられると、サーバ識別子3101に対応する保持した認証チケットデータ8112を、第１の送受信手段311を介して認証チケットTicket805として認可サーバ手段83に送る（ＳＴ８１０７）。

【００１５】認可サーバ手段83においては、認可要求Authorize Request804は第３の送受信手段331を介して認証済み証明情報8308として証明情報復号手段833に送られ、認証チケットTicket805は第３の送受信手段331を介して認証チケットデータ8301としてチケット復号手段831に送られる（ＳＴ８３０１）。チケット復号手段831は、認証チケットデータ8301を内部に保持した自サーバ共通鍵を用いて復号化して、得られたユーザ識別子8302とサーバ識別子8303とタイムスタンプ8304とをチケット有効判定手段832に送り、セッション鍵8305を証明情報復号手段833に送る（ＳＴ８３０２）。認可計時手段332は、現在時刻を計時しており、現在時刻情報8306をチケット有効判定手段832及び証明情報有効判定手段834に供給している。チケット有効判定手段832は、サーバ識別子8303と内部に保持した自サーバ識別子との一致判定を行なうとともに、タイムスタンプ8304と現在時刻情報8306との差が所定の有効期限の範囲内であることをチェックして、いずれも真である場合にユーザ識別子8302をチケットユーザ識別子8307として認可照合手段835に送る（ＳＴ３３０６、　ＳＴ３３０７）。証明情報復号手段833は、認証済み証明情報8308をセッション鍵8305を用いて復号化して、得られたユーザ識別子8309とタイムスタンプ8310とを証明情報有効判定手段834に送る（ＳＴ８３０３）。認証済み証明情報はクライアント手段でセッション鍵を用いて暗号化されているので、クライアント手段で正しいセッション鍵が用いられた場合にのみ、ここで正しいユーザ識別子とタイムスタンプとが得られる。証明情報有効判定手段834は、タイムスタンプ8310と現在時刻情報8306との差が所定の時間差の範囲内であることをチェックして、真である場合にユーザ識別子8309を証明ユーザ識別子8311として認可照合手段835に送る（ＳＴ８３０４、ＳＴ８３０５）。認可照合手段835は、チケットユーザ識別子8307と証明ユーザ識別子8311との一致判定を行ない（ＳＴ８３０６）、真であるならば認可通知8312を、第３の送受信手段331を介して認可通知Result806としてクライアント手段81に送り（ＳＴ８３０７、ＳＴ３３１７）、クライアント手段81において受信される（ＳＴ３１１８）。このとき、一致判定が真となった場合、ユーザ識別子とタイムスタンプとが正しく得られており、これはクライアント手段で正しいセッション鍵が用いられたことを示しており、これは正しいパスワードが入力されたことを意味するので、ユーザ認証結果と利用認可結果とが一致することになる。

【００１６】

【発明が解決しようとする課題】しかしながら、上記従来の構成では、多大な計算量を必要とする暗号処理を多用しており、特に利用認可処理のたびにクライアント側で暗号処理を行なう必要があるため、クライアント側が携帯型情報端末やスマートフォンのような計算処理能力の低い装置である場合には、実用的な処理時間で利用認可処理を行なうことが困難であるという課題を有していた。

【００１７】また、上記従来の構成では、１つの認証チケットの使用回数を制限しておらず有効期限を設けているのみであるため、第三者により盗聴された認証チケットの暗号が万一解読されて不正なアクセスが行なわれたとしても、発見されずに終わってしまう可能性が高いという課題も有していた。

【００１８】本発明は、こうした従来の課題を解決するものであり、クライアント側での暗号処理を必要とせず、計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができ、認証チケットの使用回数を容易に管理することができる、シングルサインオン型の認証方法及び認証システムを提供することを目的とする。

【００１９】

【課題を解決するための手段】この課題を解決するために、本発明は、第１に、有効回数がｎ（ｎは正整数）である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて提示情報を要求し前記認証チケットと照合して利用認可する認可サーバ手段と設け、前記認証チケットは、チケット識別子と照合情報と有効回数と発行日時とサーバ識別子とを含み認証子が付与されたものであり、前記照合情報は、前記認

証チケットの発行者と前記クライアント手段とが共有する秘密情報に所定の不可逆演算をｎ回施したものであり、前記認証チケットの使用回数がｋ（ｋはｎ以下の正整数）であるときの前記提示情報は、前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施したものであることを特徴としている。

【００２０】これにより、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【００２１】第２に、前記認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求するものであり、前記秘密情報は、前記ユーザ認証情報と前記乱数との連結に前記所定の不可逆演算を１回以上施したものであり、前記認証提示情報は、前記秘密情報に前記所定の不可逆演算をｎ回施したものであることを特徴としている。

【００２２】これにより、上記効果に加えて、ユーザ認証手順においてもクライアント側での暗号処理を必要としないうえ、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【００２３】第３に、前記認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求するものであり、前記認証提示情報は、前記ユーザ認証情報及び前記乱数との連結に前記所定の不可逆演算を１回以上施したものとクライアント手段が生成した認証用乱数との排他的論理和演算結果であり、前記秘密情報は、前記認証提示情報から逆算される前記認証用乱数であることを特徴としている。

【００２４】これにより、上記効果に加えて、認証チケットに含まれる照合情報がユーザ認証情報と無関係となるため認証チケットからユーザ認証情報が推測される可能性すらない、より安全なシングルサインオン型の認証方法及び認証システムが得られる。

【００２５】第４に、前記所定の不可逆演算が一方向性ハッシュ演算であることを特徴としている。

【００２６】これにより、上記効果に加えて、クライアント側が計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができる、シングルサインオン型の認証方法及び認証システムが得られる。

【００２７】第５に、前記認証チケットは発行者識別子を含み、前記認可サーバ手段は、利用認可するとともに前記認証チケットの照合情報と有効回数と発行日時と発行者識別子と認証子とを更新するものであり、前記照合情報は、前記秘密情報に前記所定の不可逆演算をｎ－ｋ回施したもので更新され、前記有効回数は、ｎ－ｋで更新されることを特徴としている。

【００２８】これにより、上記効果に加えて、認証チケットは使用するごとに更新され、特にタイムスタンプが更新されるため有効判定における有効期限をより短く設定できるので、第三者による不正使用の可能性をより小さくでき、さらに利用認可の応答時間を短縮できる、シングルサインオン型の認証方法及び認証システムが得られる。

【００２９】第６に、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認可サーバ手段を複数備え、前記認証チケットの使用回数を管理する認証チケット管理手段を備えており、前記認証サーバ手段は、前記認証チケットを発行するとともに前記認証チケット管理手段に前記認証チケットの発行登録を指示し、前記認可サーバ手段は、前記認証チケットの提示を受けて前記認証チケット管理手段に前記認証チケットの履歴更新を指示し、前記認証チケット管理手段より拒絶通知を受けた場合には利用認可しないことを特徴としている。

【００３０】これにより、上記効果に加えて、認証チケットが更新されないシステムにおいて、認証チケットを複数の認可サーバに対して共通に用いることが可能となるため、より利便性の高い、シングルサインオン型の認証方法及び認証システムが得られる。

【００３１】第７に、前記クライアント手段は、前記認証チケットの使用回数を管理しており、前記認証チケットとともにこれを示して利用認可を求めるものであり、前記認可サーバ手段を複数備え、前記認証サーバ手段は、前記認証チケットを発行するとともに発行履歴を記憶し、前記認可サーバ手段は、前記認証チケットを更新するとともに更新履歴を記憶し、前記認証チケットの提示を受けて前記認証チケットの発行者識別子が示す前記認証サーバ手段または前記認可サーバ手段に前記認証チケットの履歴を照会し、前記認証サーバ手段または前記認可サーバ手段より拒絶通知を受けた場合には利用認可しないことを特徴としている。

【００３２】これにより、上記効果に加えて、認証チケットが更新されるシステムにおいて、認証チケットの利用を分散管理できるため１個所の管理リソースをより少なくできる、シングルサインオン型の認証方法及び認証システムが得られる。

【００３３】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【００３４】（第１の実施の形態）第１の実施形態の認証システムは、図１に示すように、ユーザインタフェースを持つクライアント手段１と、ユーザ認証を行なう認証サーバ手段２と、クライアント手段１のアクセス権限を判断して利用認可を行なう認可サーバ手段３とから成る。クライアント手段１には、例えば汎用コンピュータ、携帯情報端末、スマートフォンなどが使用でき、認証サーバ手段２には、例えば汎用コンピュータ、専用認

証サーバ装置などが使用でき、また、認可サーバ手段３には、汎用コンピュータ、専用認可サーバ装置、専用情報提供装置などが使用できる。

【００３５】クライアント手段１と認可サーバ手段３との間は有線または無線通信ネットワークにより接続される。クライアント手段１と認証サーバ手段２との間は必ずしも通信ネットワークで接続されていないが、秘密情報４を共有している必要がある。この秘密情報４としては、例えばパスワード、共通鍵方式暗号鍵、またはそれらから算出される計算値などが用いられる。

【００３６】クライアント手段１は、利用認可手順で用いる認証チケット５を保持している。これは認証サーバ手段２がクライアント手段１に対して発行したものであり、認証サーバ手段２は、秘密情報４に不可逆演算ｆをｎ回（ｎは認証チケットの有効回数）行なった結果を照合情報とし、これに認証子を付加して認証チケット５を生成する。認証子は認証チケットの改ざん防止と発行者の証明とを目的として付加されるもので、メッセージ認証コードやデジタル署名などが使用できる。

【００３７】クライアント手段１と認可サーバ手段３との利用認可手順においては、クライアント手段１が秘密情報４に不可逆演算ｆをｎ－ｋ回（ｋは認証チケットの利用認可手順での使用回数）行なった結果を提示情報６として用いる。不可逆演算ｆが充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報６は秘密情報４を知らない第三者には計算することができないため、この提示情報６により秘密情報４を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算ｆの回数が多く行なわれているため、この提示情報６から次の提示情報を計算することもできないので、暗号化の必要もない。

【００３８】クライアント手段１は、この提示情報６を、保持していた認証チケット７とともに認可サーバ手段３に送り、これに対し認可サーバ手段３は、認証チケット７が含む認証子の検証と、提示情報６に不可逆演算ｆをｋ回行なった結果が認証チケット７が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知８を送り返す。

【００３９】この方法により、クライアント手段１は秘密情報４を認可サーバ手段３を含めた第三者に明かすことなく、ｎ回まで認証チケット７を使用して利用認可を得ることができる。

【００４０】このように、本実施の形態の認証システムは、有効回数がｎ（ｎは正整数）である認証チケットを保持し、これを示して利用認可を求めるクライアント手段と、これを受けて提示情報を要求し前記認証チケットと照合して利用認可する認可サーバ手段とを具備している。

【００４１】前記認証チケットには、照合情報の他に、チケット識別子、有効回数、発行日時、サーバ識別子などの情報を含めることができ、これに認証子が付与される。照合情報は、認証チケットの発行者とクライアント手段とが共有する秘密情報に所定の不可逆演算をｎ回施した情報である。また、前記提示情報は、認証チケットの使用回数がｋ（ｋはｎ以下の正整数）であるとき、前記秘密情報に所定の不可逆演算をｎ－ｋ回施した情報である。

【００４２】こうした構成により、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【００４３】（第２の実施の形態）第２の実施形態の認証システムでは、クライアント手段が、認証サーバ手段22に対して認証提示情報を示して認証チケットを要求する。

【００４４】この認証システムは、図２に示すように、ユーザインタフェースを持つクライアント手段11と、ユーザ認証を行なう認証サーバ手段12と、クライアント手段11のアクセス権限を判断して利用認可を行なう認可サーバ手段３とから成り、クライアント手段11と認証サーバ手段12及び認可サーバ手段３との間は有線または無線通信ネットワークにより接続されている。この認可サーバ手段３は第１の実施形態（図１）と同一であり、また、認証サーバ手段12からクライアント手段11に送り返される認証チケット、クライアント手段11が認可サーバ手段３に送信する提示情報及び認可チケット、さらに認可サーバ手段３からクライアント手段11に送り返される認可通知８についても、第１の実施形態（図１）と同一である。

【００４５】この認証システムのクライアント手段11と認証サーバ手段12とは、ユーザインタフェースを介して入力されたパスワードＰＷと認証サーバ手段12より得た乱数Ｒとの連結に不可逆演算ｆを１回行なった結果を秘密情報14として共有する。不可逆演算ｆが充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この秘密情報14はパスワードＰＷを知らない第三者には計算することができない。

【００４６】クライアント手段11と認証サーバ手段12とのユーザ認証手順においては、認証サーバ手段12が乱数を生成し、これを示してクライアント手段11に認証提示情報を要求する。クライアント手段11は、パスワードＰＷと認証サーバ手段12より得た乱数Ｒとの連結に不可逆演算ｆを１回行なって秘密情報14を算出し、この秘密情報14にさらに不可逆演算ｆをｎ回（通算ｎ＋１回、ｎは認証チケットの有効回数）行なった結果を認証提示情報13として認証サーバ手段12に送る。

【００４７】これに対し、認証サーバ手段12は、認証提示情報13から秘密情報14が一致していることを確認すると、秘密情報14に不可逆演算ｆをｎ回行なった結果を照合情報として、これに認証子を付加した認証チケット５

を送り返す。クライアント手段11は、これを利用認可手順で用いるために保持する。認証子は認証チケットの改ざん防止と発行者の証明を目的として付加されるもので、メッセージ認証コードやデジタル署名などが使用できる。

【００４８】また、クライアント手段11と認可サーバ手段３との利用認可手順においては、クライアント手段11が秘密情報14に不可逆演算ｆをｎ－ｋ回（ｋは認証チケットの利用認可手順での使用回数）行なった結果を提示情報６として用いる。不可逆演算ｆが充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報６は秘密情報14を知らない第三者には計算することができないため、この提示情報６により秘密情報14を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算ｆの回数が多く行なわれているため、この提示情報６から次の提示情報を計算することもできないので、暗号化の必要もない。

【００４９】クライアント手段11は、この提示情報６を、保持していた認証チケット７とともに認可サーバ手段３に送り、これに対し認可サーバ手段３は認証チケット７が含む認証子の検証と、提示情報６に不可逆演算ｆをｋ回行なった結果が認証チケット７が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知８を送り返す。

【００５０】この方法により、クライアント手段11は秘密情報14やパスワードＰＷを認可サーバ手段３を含めた第三者に明かすことなく、ｎ回まで認証チケット７を使用して利用認可を得ることができる。

【００５１】このように、本実施の形態の認証システムでは、認証サーバ手段が、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求する。このときの秘密情報として、ユーザ認証情報と乱数との連結に所定の不可逆演算を１回以上施したものを使用し、認証提示情報として、この秘密情報に所定の不可逆演算をｎ回施したものが提示される。

【００５２】こうした構成により、第１の実施形態の効果に加えて、ユーザ認証手順においてもクライアント側での暗号処理が不要であり、また、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【００５３】（第３の実施の形態）第３の実施形態の認証システムでは、図３に示すように、クライアント手段21によって生成された認証用乱数が秘密情報24としてクライアント手段21と認証サーバ手段22との間で共有される。

【００５４】このシステムでは、ユーザ認証手順において、認証サーバ手段22が乱数を生成し、これを示してクライアント手段21に認証提示情報を要求する。クライアント手段21は、パスワードＰＷと認証サーバ手段22より得た乱数Ｒとの連結に不可逆演算ｆを１回行なった結果とクライアント手段21が秘密裏に生成した秘密情報24との排他的論理和結果を認証提示情報23として認証サーバ手段22に送る。図３において、記号「＠」は排他的論理和（ＥＸＯＲ）演算を示している。

【００５５】これに対し、認証サーバ手段22は、認証提示情報23とパスワードＰＷと乱数Ｒとから逆算して秘密情報25を求める。そして、この秘密情報25に不可逆演算ｆをｎ回行ない、その演算結果を照合情報とし、これに認証子を付加した認証チケット５をクライアント手段21に送り返す。クライアント手段21は、これを利用認可手順で用いるために保持する。

【００５６】なお、もしユーザが不正な第三者で認証提示情報23が適当に作られたものだとすれば、クライアント手段21で認証チケット５を入手することができても、サーバが認証提示情報23からパスワードＰＷと乱数Ｒとを用いて逆算した秘密情報25はクライアント手段21には分からない。そのため、後続の利用認可手順においてその不正なアクセスを排除することができる。

【００５７】クライアント手段21と認可サーバ手段３との利用認可手順においては、クライアント手段21が秘密情報24に不可逆演算ｆをｎ－ｋ回（ｋは認証チケットの利用認可手順での使用回数）行なった結果を提示情報６として用いる。不可逆演算ｆが充分安全な不可逆性と結果の長さ及びランダム性を持っている限り、この提示情報６は秘密情報24を知らない第三者には計算することができないため、この提示情報６により秘密情報24を知る正当なユーザであることが示される。また、過去にさかのぼるほど提示情報における不可逆演算ｆの回数が多く行なわれているため、この提示情報６から次の提示情報を計算することもできないので、暗号化の必要もない。

【００５８】クライアント手段21は、この提示情報６を、保持していた認証チケット７とともに認可サーバ手段３に送り、これに対し認可サーバ手段３は認証チケット７が含む認証子の検証と、提示情報６に不可逆演算ｆをｋ回行なった結果が認証チケット７が含む照合情報に一致することの確認とを行なって、正当と認めれば認可通知８を送り返す。

【００５９】この方法により、クライアント手段21は、秘密情報24やパスワードＰＷを認可サーバ手段３を含めた第三者に明かすことなく、ｎ回まで認証チケット７を使用して利用認可を得ることができる。

【００６０】このように、本実施の形態の認証システムでは、認証サーバ手段は、ユーザ認証手順において乱数を生成し、これを示してクライアント手段に認証提示情報を要求する。認証提示情報は、ユーザ認証情報及び前記乱数との連結に所定の不可逆演算を１回以上施したものと、クライアント手段が生成した認証用乱数（秘密情報）との排他的論理和演算結果であり、この秘密情報は、認証サーバ手段により認証提示情報から逆算され

る。

【００６１】こうした構成により、認証チケットが含む照合情報がユーザ認証情報と無関係となる。そのため認証チケットからユーザ認証情報が推測される可能性すらないより安全な、シングルサインオン型の認証方法及び認証システムが得られる。

【００６２】（第４の実施の形態）第４の実施形態では、第２の実施形態の認証システムにおける具体的な通信手順とそれを実行する各手段のブロック構成について説明する。

【００６３】図４は、このシステムでのプロトコルを示すプロトコルシーケンス図である。図４において、31はユーザインタフェースを持つクライアント手段、32はユーザ認証を行なう認証サーバ手段、33はアクセス権限を判断して利用認可を行なう認可サーバ手段を示し、記号「Ｓ(Ｋ｜～)」は鍵Ｋを用いた認証子添付関数を示している。

【００６４】クライアント手段31と認証サーバ手段32とのユーザ認証手順においては、まず、クライアント手段31が、ユーザインタフェースを介して入力されたユーザ識別子ＵＩＤとサーバ識別子ＳＩＤとをともなった認証要求Authenticate Request301を認証サーバ手段32に送る。この時、認証要求Authenticate Request301が認証チケットの有効回数ｎをともなうものとしてもよい。そうでない場合には、認証サーバが固定的に有効回数ｎを定めるものとすればよい。

【００６５】これに対して、認証サーバ手段32は、毎回異なるように生成された乱数ＲＯをともなった認証チャレンジChallenge302を送り返す。これを受けたクライアント手段31は、ユーザインタフェースを介して入力されたパスワードＰＷと乱数ＲＯとの連結に対してｎ＋１段のハッシュ演算Ｈを施した結果をともなった認証チャレンジ応答Response303を送り返し、これに対し認証サーバ手段32は、チャレンジ応答Response303におけるｎ＋１段ハッシュ演算結果と自ら行なったｎ＋１段ハッシュ演算結果とを比較検証して一致すれば正当と認め、新たに生成したチケット識別子ＴＩＤとｎ＋１段ハッシュ演算結果とタイムスタンプＴＳＯとサーバ識別子ＳＩＤと認証サーバ32自身を示す発行者識別子ＩＩＤとをともない認証子が付加された認証チケットTicket304を送り返す。クライアント手段31は、これを利用認可手順で用いるために保持する。

【００６６】また、クライアント手段31と認可サーバ手段33との利用認可手順においては、クライアント手段31が認可要求Authorize Request及び認証チケットTicket305を認可サーバ手段33に送る。この時、認可要求Authorize Requestがユーザ識別子ＵＩＤをともなうものとしてもよい。これに対して、認可サーバ手段33は、この認証チケットの使用回数に基づく値ｋをともなった認可チャレンジChallenge306を送り返す。これを受けたクライアント手段31は、パスワードＰＷと乱数ＲＯとの連結にｎ－ｋ＋１段のハッシュ演算Ｈを施した結果をともなった認可チャレンジ応答Response307を送り返す。

【００６７】このハッシュ演算Ｈが充分安全な一方向性と結果の長さ及びランダム性を持っている限り、このハッシュ演算結果はパスワードＰＷ及び乱数ＲＯを知らない第三者には計算することができないため、このハッシュ演算結果によりパスワードＰＷを知る正当なユーザであることが示される。また、過去にさかのぼるほどハッシュ演算Ｈの段数が多く行なわれているため、このハッシュ演算結果から次のハッシュ演算結果を計算することもできないので、暗号化の必要もない。このようなハッシュ演算Ｈとしては、例えばＭＤ５やＳＨＡなどのアルゴリズムを使用することができる。

【００６８】これに対して、認可サーバ手段32は、認可チャレンジ応答Response307におけるｎ－ｋ＋１段ハッシュ演算結果にさらにｋ段のハッシュ演算を施した結果と認証チケットTicketにおけるｎ＋１段ハッシュ演算結果とを比較検証し、一致すれば正当と認めて認可通知Result308を送り返す。この時、認可通知308が利用認可によりアクセスが許可された情報Infoを同時にともなうものとしてもよい。

【００６９】以上のようなプロトコルシーケンスにより、クライアント手段31はパスワードＰＷを認可サーバ手段33を含めた第三者に明かすことなく、ｎ回まで認証チケット304を使用して利用認可を得ることができる。

【００７０】このようなプロトコルシーケンスを持つ認証システムの構成について図５の機能ブロック図を参照しながら説明する。

【００７１】図５において、31はユーザインタフェースを持つクライアント手段、32はユーザ認証を行なう認証サーバ手段、33はアクセス権限を判断して利用認可を行なう認可サーバ手段である。

【００７２】クライアント手段31は、データの送受信を行なう第１の送受信手段311と、ユーザからの入力を得る入力手段312と、２つの入力を連結してハッシュ演算Ｈを行なうハッシュ手段313と、受信した認証チケットを保持するチケット保持手段314と、認証チケットの保持状態に応じて処理を選択する処理選択手段315と、ハッシュ演算結果を秘密裏に記憶する機密記憶手段316と、与えられた段数または与えられた２つの数値の差の段数のハッシュ演算を行なう多段ハッシュ手段317とを備えている。

【００７３】第１の送受信手段311は、通信ネットワークの種類に応じて例えばＬＡＮカード等のＬＡＮインタフェース装置、ターミナルアダプタ等のＩＳＤＮインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやＰＩＡＦＳカード等の無線インタフェース装置、ＩｒＤＡモジュール等の赤外線インタフェース装置などで構成され、通信相手に応じてこれらの

いくつかを使い分ける構成としてもよい。入力手段312は、例えばキーボード、テンキー等の文字入力装置、マウス、トラックボール、ペンタブレット等のポインティングデバイスや選択ボタンやダイヤルと表示画面との組合せ、あるいはタッチパネルなどで構成される。ハッシュ手段313は、例えば論理回路とハッシュ演算Ｈのアルゴリズムを組み込んだ演算回路とを組み合わせて構成される。チケット保持手段314は、例えばメモリ回路が使用される。処理選択手段315は、例えば論理回路が使用できる。機密記憶手段316は、例えばＩＣカードのような耐タンパ性を持ったメモリデバイスによって構成される。多段ハッシュ手段317は、例えばハッシュ演算Ｈのアルゴリズムを組み込んだ演算回路に出力をフィードバックする結線や段数をカウントするカウンタや数値の差を求める演算回路などを追加して構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【００７４】また、認証サーバ手段32は、データの送受信を行なう第２の送受信手段321と、現在時刻を計時する認証計時手段322と、パスワード等のユーザ認証情報を蓄積する認証情報蓄積手段323と、ユーザ認証処理毎に乱数を生成する乱数生成手段324と、与えられたよりも１多い段数のハッシュ演算Ｈを行なう第２の多段ハッシュ手段325と、２つの多段ハッシュ値を比較照合する認証照合手段326と、認証チケット発行毎にユニークなチケット識別子を生成するチケット識別子生成手段327と、認証チケットに対する認証子を生成して付加する認証子付加手段328とを備えている。

【００７５】第２の送受信手段321は、通信ネットワークの種類に応じて例えばＬＡＮカード等のＬＡＮインタフェース装置、ターミナルアダプタ等のＩＳＤＮインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやＰＩＡＦＳカード等の無線インタフェース装置、ＩｒＤＡモジュール等の赤外線インタフェース装置などで構成される。認証計時手段322は、例えばタイマカウンタが使用される。認証情報蓄積手段323は、大容量のメモリデバイスで構成され、耐タンパ性を持ったメモリデバイスであればなお良い。乱数生成手段324は、例えば乱数生成アルゴリズムを組み込んだ演算回路、あるいは電磁的ノイズをデータ化する変換装置などで構成される。第２の多段ハッシュ手段325は、例えばハッシュ演算Ｈのアルゴリズムを組み込んだ演算回路に出力をフィードバックする結線や段数をカウントするカウンタなどを追加して構成される。認証照合手段326は、例えば比較回路で構成される。チケット識別子生成手段327は、例えば充分なビット長を持ったカウンタ回路で構成される。認証子付加手段328は、認証子生成アルゴリズムを組み込んだ演算回路及びメモリ回路で構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【００７６】また、認可サーバ手段33は、データの送受信を行なう第３の送受信手段331と、現在時刻を計時する認可計時手段332と、認証チケットに付加された認証子を検証する認証子検証手段333と、認証チケットの有効性判定を行なうチケット有効判定手段334と、認証チケットのチケット識別子と有効回数と残り利用可能回数を管理するチケット利用管理手段335と、与えられた段数のハッシュ演算Ｈを行なう第３の多段ハッシュ手段336と、２つの多段ハッシュ値を比較照合する認可照合手段337とを備えている。

【００７７】第３の送受信手段331は、通信ネットワークの種類に応じて例えばＬＡＮカード等のＬＡＮインタフェース装置、ターミナルアダプタ等のＩＳＤＮインタフェース装置、モデム等の電話インタフェース装置、携帯データ通信カードやＰＩＡＦＳカード等の無線インタフェース装置、ＩｒＤＡモジュール等の赤外線インタフェース装置などで構成される。認可計時手段332は、例えばタイマカウンタが使用される。認証子検証手段333は、認証子検証アルゴリズムを組み込んだ演算回路及びメモリ回路で構成される。チケット有効判定手段334は、例えば比較回路の組合せにより構成される。チケット利用管理手段335は、利用回数を計算する演算回路と大容量のメモリデバイスとの組合せにより構成される。第３の多段ハッシュ手段336は、例えば第２の多段ハッシュ手段325と同様の演算回路でカウンタのプリセット値を改めもので構成される。認可照合手段337は、例えば比較回路で構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【００７８】以上のように構成された認証方法及び認証システムにおいて、以下その動作について図６を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数ｎをともなう場合について説明する。

【００７９】まず、クライアント手段31において、ユーザ自身を示すユーザ識別子ＵＩＤと認証サーバ手段32にあらかじめ登録されたユーザ認証用のパスワードＰＷと利用認可を得る対象のサーバ識別子ＳＩＤと認証チケットの有効回数ｎとがユーザ入力300として入力手段312に

入力される（ＳＴ３１０１、　ＳＴ３１０４）。入力手段312は、ユーザ入力300を一時保持するとともにサーバ識別子3101を取出してチケット保持手段314に送る。チケット保持手段314は、サーバ識別子3101に対応する認証チケットデータを検索して（ＳＴ３１０２）、検索結果通知3102を処理選択手段315に送る。処理選択手段315は、検索結果通知3102が無しを示す場合には、ユーザ認証処理起動通知3103を前記入力手段312及び多段ハッシュ手段317に送り、有りを示す場合には（ＳＴ３１０３）、利用認可手順起動通知3104を前記チケット保持手段314と機密記憶手段316と多段ハッシュ手段317とに送る。

【００８０】前記入力手段312は、ユーザ認証起動通知3103が与えられると、一時保持したユーザ入力300から取出した、ユーザ識別子とサーバ識別子と有効回数の組3105を第１の送受信手段311を介して認証要求Authenticate Request301として認証サーバ手段32に送り（ＳＴ３１０５）、有効回数3106を多段ハッシュ手段317に送り、パスワード3107をハッシュ手段313に送る。

【００８１】認証サーバ手段32においては、認証要求Authenticate Request301は第２の送受信手段321で受信され、取出されたユーザ識別子3201が認証情報蓄積手段323に送られ、有効回数3202が第２の多段ハッシュ手段325及び認証子付加手段328に送られ、サーバ識別子3203が認証子付加手段328に送られる（ＳＴ３２０１）。認証情報蓄積手段323は、ユーザ識別子3201に対応するパスワードを検索して（ＳＴ３２０２）、有りの場合には（ＳＴ３２０３）、パスワード3204を第２の多段ハッシュ手段325に送り、検索結果通知3205を乱数生成手段324及び第２の多段ハッシュ手段325に送る。

【００８２】乱数生成手段324は、検索結果通知3205が有りを示す場合に、データ撹乱用のチャレンジ乱数3206を新たにランダムに生成して第２の多段ハッシュ手段325に送るとともに、第２の送受信手段321を介して認証チャレンジChallenge302としてクライアント手段31に送る（ＳＴ３２０４）。第２の多段ハッシュ手段325は、検索結果通知3205が有りを示す場合に、パスワード3204とチャレンジ乱数3206との連結に対し有効回数3202より１多い段数のハッシュ演算Ｈを行なって、結果の多段ハッシュ値3207を認証照合手段326に送る（ＳＴ３２０５）。

【００８３】これに対してクライアント手段31においては、認証チャレンジChallenge302は第１の送受信手段311で受信され、チャレンジ乱数3108が取り出されてハッシュ手段313に送られる（ＳＴ３１０６）。ハッシュ手段313はパスワード3107とチャレンジ乱数3108との連結に対するハッシュ演算Ｈを行なって（ＳＴ３１０７）、結果のハッシュ値3109を機密記憶手段316及び多段ハッシュ手段317に送る。機密記憶手段316はハッシュ値3109を秘密裏に記憶して所定のアクセスのみ、すなわちユーザ認証手順における追加更新及び利用認可手順における参照のみ許容する（ＳＴ３１０８）。多段ハッシュ手段317は、ユーザ認証手順起動通知3103が与えられている時、ハッシュ値3109に有効回数3106に相当する段数のハッシュ演算Ｈを行なって（ＳＴ３１０９）、結果の多段ハッシュ値3114を、第１の送受信手段311を介して認証チャレンジ応答Response303として認証サーバ手段32に送る（ＳＴ３１１０）。

【００８４】これに対して認証サーバ手段32においては、認証チャレンジ応答Response303は第２の送受信手段321で受信され、多段ハッシュ値3208が取出されて認証照合手段326に送られる（ＳＴ３２０６）。認証照合手段326は、多段ハッシュ値3207と多段ハッシュ値3208との一致判定を行ない（ＳＴ３２０７）、照合結果3209をチケット識別子生成手段327に送るとともに多段ハッシュ値3208をそのまま多段ハッシュ値3210として認証子付加手段328に送る。チケット識別子生成手段327は、照合結果327が一致を示す場合に、有効なチケット識別子3212を生成して認証子付加手段328に送る（ＳＴ３２０８）。

【００８５】認証計時手段322は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3211を認証子付加手段328に供給している。認証子付加手段328は、チケット識別子3212と多段ハッシュ値3210と有効回数3202とタイムスタンプ3211とサーバ識別子3203と認証サーバ32自身を示す発行者識別子とを連結し、これに対して認証子を生成して付加して認証チケットデータ3213とし（ＳＴ３２０９）、第２の送受信手段321を介して認証チケットTicket304としてクライアント手段31に送る（ＳＴ３２１０）。

【００８６】これに対してクライアント手段31においては、認証チケットTicket304は第１の送受信手段311で受信され、認証チケットデータ3110が取出されて前記チケット保持手段314に送られる（ＳＴ３１１１）。前記チケット保持手段314は認証チケットデータ3110をサーバ識別子3101と対応づけて保持し（ＳＴ３１１２）、利用認可手順起動通知3104が与えられた場合に、認証チケットデータ3111を第１の送受信手段311を介して認証チケットTicket305として認可要求Authorize Requestとともに認可サーバ手段33に送る（ＳＴ３１１３）とともに、認証チケットデータから有効回数3112を取出して多段ハッシュ手段317に送る。

【００８７】これに対して認可サーバ手段33においては、認証チケットTicket305をともなった認可要求Authorize Requestは第３の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られる（ＳＴ３３０１）。認証子検証手段333は、認証チケットデータ3301の認証子と認証子以外のデータ部との整合性を検証して検証結果3304をチケット有効判定手段334に送るとともに（ＳＴ３３０４）、データ部か

らタイムスタンプ3302とサーバ識別子3303とを取出してチケット有効判定手段334に、チケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とを取出してチケット利用管理手段335に、それぞれ送る。

【００８８】認可計時手段332は、現在時刻を計時しており、現在時刻に基づくタイムスタンプ3309をチケット有効判定手段334に供給している。チケット有効判定手段334は、検証結果3304が誤りなしを示す場合に（ＳＴ３３０５）、サーバ識別子3303と内部に保持した自サーバ識別子との一致判定を行なうとともに（ＳＴ３３０２、ＳＴ３３０３）、タイムスタンプ3302と現在時刻に基づくタイムスタンプ3309との差が所定の有効期限の範囲内であることをチェックして（ＳＴ３３０６、ＳＴ３３０７）、いずれも真である場合にチケット有効通知3310をチケット利用管理手段335に送る。この有効期限は、短く設定するとセキュリティは向上するがユーザ利便性は低下し、長く設定するとユーザ利便性は向上するがセキュリティは低下するため、これらのバランスを勘案して定めるべきである。例えば厳重なセキュリティまでは要求されていない業務用システムに適用するならば１日の勤務時間をカバーできる８時間なり１２時間なりにすればよい。ただし、最短でもクライアント～サーバ間の通信時間及び各計時手段の間の時刻誤差をカバーできる必要がある。

【００８９】このとき、チケット利用管理手段335はチケットリストを管理しており、チケット有効通知3310が与えられた場合に、チケット識別子3305を用いてチケットリスト中を検索して既に登録されているかを調べる（ＳＴ３３０８）。該当するものが無ければチケット識別子3305と有効回数3307と残り利用可能回数とを示す値としての有効回数3307の組をチケットリストに追加し記憶する（ＳＴ３３０９、ＳＴ３３１０）。この時、多段ハッシュ値3306と発行者識別子3308をあわせて記憶してもよい。この追加した組、あるいは検索で該当するものがあった場合は当該の組みに対し、チケット利用管理手段335は残り利用可能回数を１減じ、有効回数と残り利用可能回数との差が示す利用回数3311を求め（ＳＴ３３１１）、これを第３の送受信手段331を介して認可チャレンジChallenge306としてクライアント手段31に送るとともに（ＳＴ３３１２）、第３の多段ハッシュ手段336にも送る。また、多段ハッシュ値3306をそのまま多段ハッシュ値3312として認可照合手段337に送る。

【００９０】これに対してクライアント手段31においては、認可チャレンジChallenge306は第１の送受信手段311で受信され、利用回数3115が取出されて多段ハッシュ手段317に送られる（ＳＴ３１１４）。多段ハッシュ手段317は、利用認可手順起動通知3104が与えられている場合に、前記機密記憶手段316よりハッシュ値3113を得て（ＳＴ３１１５）、ハッシュ値3113に有効回数3112と利用回数3115との差に相当する段数のハッシュ演算Ｈを行なって（ＳＴ３１１６）、結果の多段ハッシュ値3116を、第１の送受信手段311を介して認可チャレンジ応答Response307として認可サーバ手段33に送る（ＳＴ３１１７）。

【００９１】ハッシュ演算Ｈが充分安全な一方向性と結果の長さ及びランダム性を持っている限り、この多段ハッシュ値3116はパスワードＰＷ及び乱数Ｒ０を知らない第三者には計算することができないため、この多段ハッシュ値3116によりパスワードＰＷを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Ｈの段数が多く行なわれているため、この多段ハッシュ値3116から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも１００倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【００９２】これに対して認可サーバ手段33においては、認可チャレンジ応答Response307は第３の受信手段331で受信され、多段ハッシュ値3313が取出されて第３の多段ハッシュ手段336に送られる（ＳＴ３３１３）。第３の多段ハッシュ手段336は、多段ハッシュ値3313に利用回数3311に相当する段数のハッシュ演算Ｈを行なって、結果の二次多段ハッシュ値3314を認可照合手段337に送る（ＳＴ３３１４）。認可照合手段337は、多段ハッシュ値3312と二次多段ハッシュ値3314との一致判定を行ない（ＳＴ３３１５、ＳＴ３３１６）、真であるならば認可通知3315を、第３の送受信手段331を介して認可通知Result308としてクライアント手段31に送り（ＳＴ３３１７）、クライアント手段31において受信される（ＳＴ３１１８）。この方法により、クライアント手段31はパスワードＰＷを認可サーバ手段33を含めた第三者に明かすことなく、ｎ回まで認証チケット305を使用して利用認可を得ることができる。

【００９３】なお、以上の説明ではクライアント手段31において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【００９４】次に、図５に示した第４の実施形態の認証システムにおいて、認証子としてメッセージ認証コードを用いた場合の認証子付加手段328及び認証子検証手段333の詳細な構成例及び動作について、図７及び図８を参照して説明する。

【００９５】認証子付加手段328は、図７に示すように、認証サーバ自身を示す識別子が記憶された自識別子記憶手段328Aと、データを連結するデータ連結手段328B

と、ハッシュ演算ｈを行なう連結データハッシュ手段328Ｃと、認証サーバ手段31と認可サーバ手段32とが共通の秘密として持つサーバ共通鍵を記憶するサーバ共通鍵記憶手段328Dと、共通鍵方式の暗号処理を行なう共通鍵方式暗号手段328Eと、認証子をデータに連結する認証子連結手段328Fとを具備している。

【００９６】この自識別子記憶手段328Aは、例えばメモリで構成される。データ連結手段328Bは、例えば論理回路で構成できる。連結データハッシュ手段328Cは、例えばハッシュ演算ｈのアルゴリズムを組み込んだ演算回路で構成される。ここでハッシュ演算ｈは、ハッシュ演算Ｈと同じであっても異なっていても良い。サーバ共通鍵記憶手段328Dは、例えばメモリで構成され、耐タンパ性を持ったメモリデバイスであればなお良い。共通鍵方式暗号手段328Eは、例えば暗号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサで構成される。ここで暗号アルゴリズムとしては、例えばＤＥＳやトリプルＤＥＳなどが使用できる。認証子連結手段328Fは、例えば論理回路で構成される。

【００９７】また、認証子検証手段333は、図８に示すように、認証子をデータから分離する認証子分離手段333Aと、ハッシュ演算ｈを行なう第２の連結データハッシュ手段333Bと、認証サーバ手段31と認可サーバ手段32とが共通の秘密として持つサーバ共通鍵を記憶する第２のサーバ共通鍵記憶手段333Cと、共通鍵方式の暗号処理を行なう第２の共通鍵方式暗号手段333Dと、データ部を分割分離するデータ分離手段333Eと、発行者識別子を照合する発行者識別子照合手段333Fと、メッセージ認証コードを比較検証する比較手段333Gと具備している。

【００９８】この認証子分離手段333Aは、例えば論理回路で構成される。第２の連結データハッシュ手段333B、第２のサーバ共通鍵記憶手段333C及び第２の共通鍵方式暗号手段333Dは、それぞれ図７における328C、328D、328Eと同じように構成される。データ分離手段333Eは、例えば論理回路で構成される。発行者識別子照合手段333Fは、例えばメモリ回路及び比較回路で構成される。比較手段333Gは、例えば比較回路の組合せにより構成される。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【００９９】以上のように構成された認証子付加手段328及び認証子検証手段333の動作について説明する。認証子付加手段328では、まず、自識別子記憶手段328Aからデータ連結手段328Bに認証サーバ自身を示す識別子が発行者識別子328aとして供給されている。データ連結手段328Bは、第２の送受信手段321より得た有効回数3202及びサーバ識別子3203と、認証照合手段326より得た多段ハッシュ値3210と、認証計時手段322より得たタイムスタンプ3211と、チケット識別子生成手段327より得たチケット識別子3212と、自識別子記憶手段328Aより得た発行者識別子328aとを定められた順序で並べて連結し、データ部328bとして連結データハッシュ手段328C及び認証子連結手段328Fに送る。

【０１００】連結データハッシュ手段328Cは、データ部328bに対するハッシュ演算ｈを行なって、結果のハッシュ値328cを共通鍵方式暗号手段328Eに送る。共通鍵方式暗号手段328Eは、サーバ共通鍵記憶手段328Dからサーバ共通鍵328dを得て、これを暗号鍵に用いてハッシュ値328cを暗号化して、メッセージ認証コード328eとして認証子連結手段328Fに送る。認証子連結手段328Fは、データ部328bにメッセージ認証コード328eを連結して、認証チケットデータ3213を出力する。

【０１０１】また、認証子検証手段333では、まず、認証チケットデータ3301が認証子分離手段333Aに入力され、メッセージ認証コード333aとデータ部333bとに分離され、メッセージ認証コード333aは比較手段333Gに、データ部333bは第２の連結データハッシュ手段333B及びデータ分離手段333Eにそれぞれ送られる。第２の連結データハッシュ手段333Bは、データ部333bに対するハッシュ演算ｈを行なって、結果のハッシュ値333cを第２の共通鍵方式暗号手段333Dに送る。第２の共通鍵方式暗号手段333Dは、第２のサーバ共通鍵記憶手段333Cからサーバ共通鍵333dを得て、これを暗号鍵に用いてハッシュ値333cを暗号化して、比較用メッセージ認証コード333eとして比較手段333Gに送る。データ分離手段333Eは、データ部333bをタイムスタンプ3302とサーバ識別子3303とチケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とに分離して出力するとともに、発行者識別子3308については発行者識別子照合手段333Fにも送る。発行者識別子照合手段333Fは、発行者識別子3308が認証サーバ32の識別子かどうかを照合し、照合結果333fを比較手段333Gに送る。比較手段333Gは、照合結果333fが一致を示すか、メッセージ認証コード333aと比較用メッセージ認証コード333eとが一致するかをもとに検証結果3304を出力する。検証結果3304が誤りなしを示すのは、いずれも一致した場合である。

【０１０２】次に、図５の第４の実施形態の認証システムにおいて、認証子としてデジタル署名を用いた場合の認証子付加手段328及び認証子検証手段333の構成及び動作について、図９及び図１０を参照して説明する。図９において図７と異なるのは、サーバ共通鍵記憶手段328D及び共通鍵方式暗号手段328Eの代わりに、認証サーバ32自身の公開鍵方式暗号秘密鍵を記憶する自秘密鍵記憶手段328G及び公開鍵方式の暗号処理を行なう公開鍵方式暗号手段328Hを設けた点にある。自秘密鍵記憶手段328Gとしては、例えばメモリが使用でき、耐タンパ性を持ったメモリデバイスであればなお良い。公開鍵方式暗号手段

328Hとしては、例えば暗号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサが使用できる。ここで暗号アルゴリズムとしては、例えばＲＳＡや楕円曲線暗号などが使用できる。

【０１０３】また、図１０において図８と異なるのは、第２のサーバ共通鍵記憶手段333C、第２の共通鍵方式暗号手段333D及び発行者識別子照合手段333Fの代わりに、認証サーバ手段31の公開鍵をサーバ識別子と対応づけて１つ以上蓄積するサーバ公開鍵蓄積手段333H及び公開鍵方式暗号の復号処理を行なう公開鍵方式復号手段333Jを設け、これらの間の結線を改めた点にある。サーバ公開鍵蓄積手段333Hは、認証サーバ手段32のみならず認可サーバ手段33の公開鍵をも蓄積するものとしてもよい。サーバ公開鍵蓄積手段333Hとしては、例えばメモリ回路が使用でき、大容量のメモリデバイスであればなお良い。公開鍵方式復号手段333Jとしては、例えば復号アルゴリズムを組み込んだ演算回路または暗号処理専用プロセッサが使用できる。ここで復号アルゴリズムとしては、公開鍵方式暗号手段328Hにおける暗号アルゴリズムに対応する復号アルゴリズムを用いることは言うまでもない。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【０１０４】以上のように構成された認証子付加手段328及び認証子検証手段333の動作について説明する。認証子付加手段328では、自識別子記憶手段328A、データ連結手段328B、連結データハッシュ手段328Cの動作は図７の場合と同様であり、データ部328bが認証子連結手段328Fに、ハッシュ値328cが公開鍵方式暗号手段328Hに、それぞれ供給される。公開鍵方式暗号手段328Hは、自秘密鍵記憶手段328Gから自秘密鍵328fを得て、これを暗号鍵に用いてハッシュ値328cを暗号化して、デジタル署名328gとして認証子連結手段328Fに送る。認証子連結手段328Fは、データ部328bにデジタル署名328gを連結して、認証チケットデータ3213を出力する。

【０１０５】また、認証子検証手段333では、まず、認証チケットデータ3301が認証子分離手段333Aに入力され、デジタル署名333gとデータ部333bとに分離され、デジタル署名333gは公開鍵方式復号手段333Jに、データ部333bは第２の連結データハッシュ手段333B及びデータ分離手段333Eにそれぞれ送られる。第２の連結データハッシュ手段333Bは、データ部333bに対するハッシュ演算ｈを行なって、結果のハッシュ値333hを比較手段333Gに送る。データ分離手段333Eは、データ部333bをタイムスタンプ3302とサーバ識別子3303とチケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とに分離して出力するとともに、発行者識別子3308についてはサーバ公開鍵蓄積手段333Hにも送る。サーバ公開鍵蓄積手段333Hは、発行者識別子3308が既知の認証サーバ31（または認可サーバ32）の識別子かどうか検索照合し、照合結果333iを比較手段333Gに送るとともに、発行者識別子3308に対応するサーバ公開鍵333jを公開鍵方式復号手段333Jに送る。

【０１０６】公開鍵方式復号手段333Jは、サーバ公開鍵333jを復号鍵に用いてデジタル署名333gを復号化して、比較用ハッシュ値333kとして比較手段333Gに送る。比較手段333Gは、照合結果333iが一致を示すか、ハッシュ値333hと比較用ハッシュ値333kとが一致するかをもとに検証結果3304を出力する。検証結果3304が誤りなしを示すのは、いずれも一致した場合である。

【０１０７】このように、認証システムがこの実施形態の構成を採ることにより、クライアント側が計算処理能力の低い装置であっても、実用的な処理時間で利用認可処理を行なうことが可能になる。

【０１０８】（第５の実施の形態）第５の実施形態では、第３の実施形態の認証システムにおける具体的な通信手順とそれを実行する各手段のブロック構成について説明する。

【０１０９】図１１は第５の実施形態における認証システムのプロトコルを示すプロトコルシーケンス図である。図１１において図４と異なるのは、ユーザインタフェースを持つクライアント手段41とユーザ認証を行なう認証サーバ手段42とであって、認可サーバ手段33は変わりがない。また、認証チャレンジ応答Response401がユーザインタフェースを介して入力されたパスワードＰＷと乱数Ｒ０との連結に対して１段のハッシュ演算Ｈを施した結果とクライアント手段41が秘密裏に生成した認証用乱数Ｓ０との排他的論理和結果（記号「＠」は排他的論理和演算を示す）をともなう点、認証チケットTicket402、403がともなうハッシュ演算結果が認証用乱数Ｓ０に対するｎ段のハッシュ演算結果である点、認可チャレンジ応答Response404がともなうハッシュ演算結果が認証用乱数Ｓ０に対するｎ－ｋ段のハッシュ演算である点が異なる。

【０１１０】以上のようなプロトコルシーケンスにより、クライアント手段41はパスワードＰＷを認可サーバ手段33を含めた第三者に明かすことなく、ｎ回まで認証チケット402を使用して利用認可を得ることができ、認証チケット402がパスワードＰＷに無関係の内容であるため、不正な第三者によるパスワードＰＷを盗むための攻撃対象にすらならず、より安全性が高い。

【０１１１】このようなプロトコルシーケンスを持つ認証システムの構成について図１２の機能ブロック図を参照しながら説明する。

【０１１２】図１２においても図５と異なるのは、ユーザインタフェースを持つクライアント手段41及びユーザ認証を行なう認証サーバ手段42であって、認可サーバ手

段33は変わりがない。また、クライアント手段41において図５のクライアント手段31と異なるのは、ユーザ認証処理毎に乱数を生成する認証用乱数生成手段411、及びビット毎の排他的論理和演算を行なう第１の排他的論理和手段412を設け、一部の結線を改めた点にある。また、認証サーバ手段42において図５の認証サーバ手段32と異なるのは、第２の多段ハッシュ手段325、認証照合手段326の代わりに、ハッシュ演算Ｈを行なう第２のハッシュ手段421、ビット毎の排他的論理和演算を行なう第２の排他的論理和手段422、与えられた段数のハッシュ演算Ｈを行なう第２の多段ハッシュ手段423を設け、一部の結線を改めた点にある。認証用乱数生成手段411としては、例えば乱数生成アルゴリズムを組み込んだ演算回路、あるいは電磁的ノイズをデータ化する変換装置などが使用できる。第１、第２の排他的論理和手段412、422としては、例えば論理回路が使用できる。第２のハッシュ手段421としては、例えばハッシュ演算Ｈのアルゴリズムを組み込んだ演算回路が使用できる。第２の多段ハッシュ手段423としては、例えば421と同様の演算回路に出力をフィードバックする結線や段数をカウントするカウンタなどを追加して構成できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【０１１３】以上のように構成された認証システムの動作について図１３を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数ｎをともなう場合について説明する。

【０１１４】まず、クライアント手段41及び認証サーバ手段42において、第１、第２の送受信手段311、321、入力手段312、チケット保持手段314、処理選択手段315、認証情報蓄積手段323、乱数生成手段324の動作は図５、図６の場合と同様であり、認証要求Authenticate Request301及び認証チャレンジChallenge302が交換されて、クライアント手段41においてはユーザ認証処理起動通知4101または利用認可手順起動通知3104が、認証サーバ手段42においては有効回数4201とサーバ識別子3203とパスワード3204と検索結果通知4202とチャレンジ乱数3206とが得られる。ただし、ユーザ認証処理起動通知4101が前記入力手段312、認証用乱数生成手段411及び第１の排他的論理和手段412に送られる点、有効回数4201が第２の多段ハッシュ手段423及び認証子付加手段328に送られる点、検索結果通知4202が第２のハッシュ手段421、乱数生成手段324及びチケット識別子生成手段327に送られる点、チャレンジ乱数3206が第２のハッシュ手段421に送られるとともに第２の送受信手段321を介してクライアント手段41に送られる点が異なる。

【０１１５】次に、クライアント手段41において、認証用乱数生成手段411は、ユーザ認証処理起動通知4101が与えられると、認証済み証明に用いられる認証用乱数4102を新たにランダムかつ秘密裏に生成して第１の排他的論理和手段412及び機密記憶手段316に送る（ＳＴ４１０１）。機密記憶手段316は、認証用乱数4102を秘密裏に記憶して所定のアクセスのみ、すなわちユーザ認証手順における追加更新及び利用認可手順における参照のみ許容する（ＳＴ４１０２）。第１の排他的論理和手段412は、ユーザ認証処理起動通知4101が与えられると、ハッシュ手段313より得たハッシュ値4103と認証用乱数4102との間でビット毎の排他的論理和演算を行ない、結果として得られた撹乱ハッシュ値4104を第１の送受信手段311を介して認証チャレンジ応答Response401として認証サーバ手段42に送る（ＳＴ４１０３、ＳＴ４１０４）。

【０１１６】これに対して認証サーバ手段42においては、認証チャレンジ応答Response401は第２の送受信手段321で受信され、撹乱ハッシュ値4204が取出されて第２の排他的論理和手段422に送られる（ＳＴ４２０２）。一方で第２のハッシュ手段421は、検索結果通知4202が有りを示す場合に、パスワード3204とチャレンジ乱数3206との連結に対しハッシュ演算Ｈを行なって、結果のハッシュ値4203を第２の排他的論理和手段422に供給している（ＳＴ４２０１）。第２の排他的論理和手段422は、第２のハッシュ手段421より得たハッシュ値4203と撹乱ハッシュ値4204との間でビット毎の排他的論理和演算を行ない、結果として得られた認証用乱数4205を第２の多段ハッシュ手段423に送る（ＳＴ４２０３）。第２の多段ハッシュ手段423は、認証用乱数4205に対し有効回数4201相当の段数のハッシュ演算Ｈを行なって、結果の多段ハッシュ値4206を認証子付加手段328に送る（ＳＴ４２０４）。

【０１１７】以下、チケット識別子生成手段327、認証計時手段322、認証子付加手段328の動作は図４、図５の場合と同様であるが、チケット識別子生成手段327が照合結果3209の代わりに検索結果通知4202を用いる点、認証子付加手段328が有効回数3202及び多段ハッシュ値3210の代わりに有効回数4201及び多段ハッシュ値4206を用いる点が異なり、認証チケットデータ3213とは異なる内容の認証チケットデータ4207が得られ（ＳＴ４２０５）、第２の送受信手段321を介して認証チケットTicket402としてクライアント手段41に送られる。

【０１１８】これに対してクライアント手段41においては、前記第１の送受信手段311、前記チケット保持手段314が図５、図６の場合と同様に動作し、利用認可手順起動通知3104が与えられた場合に、認証チケットTicket403が認可要求Authorize Requestとともに認可サーバ手段33に送られ、有効回数3112が多段ハッシュ手段317に供給される。

【０１１９】これに対する認可サーバ手段33の動作も図５、図６の場合と同様であり、認可チャレンジChalleng

e306が返される。

【０１２０】これに対してクライアント手段41においては、前記第１の送受信手段311、多段ハッシュ手段317が図５、図６の場合と同様に動作する。ただし、前記機密記憶手段316より得るのは認証用乱数4105であり（ＳＴ４１０５）、これに対して処理が行なわれる。すなわち、多段ハッシュ手段317が有効回数3112と利用回数3115との差に相当する段数のハッシュ演算Ｈを行なって（ＳＴ４１０６）、結果の多段ハッシュ値4106を第１の送受信手段311を介して認可チャレンジ応答Response404として認可サーバ手段33に送る（ＳＴ４１０７）。

【０１２１】これにより認可サーバ手段33が得る認可チャレンジ応答Response404がともなう多段ハッシュ値、認証チケットTicket403がともなう多段ハッシュ値は、図５、図６の場合とはハッシュ対象が異なるのみであり、前者と後者の演算関係は保たれている。従って、これに対する認可サーバ手段33の動作も図５、図６の場合と同様でよく、２つの多段ハッシュ値の関係をチェックして、正当と認めれば認可通知Result308が返され、クライアント手段41において受信される。この方法により、クライアント手段41はパスワードＰＷを認可サーバ手段33を含めた第三者に明かすことなく、かつパスワードＰＷとは無関係で安全性のより高い認証チケット402を使用してｎ回まで利用認可を得ることができる。

【０１２２】なお、以上の説明ではクライアント手段41において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【０１２３】このように、認証システムがこの実施形態の構成を採ることにより、クライアント側が計算処理能力の低い装置であっても、実用的な処理時間で利用認可処理を行なうことが可能になる。また、認証チケットに含まれる照合情報がユーザ認証情報と無関係になるため、認証チケットからユーザ認証情報が推測される可能性が無くなり、より安全性の高い、シングルサインオン型の認証方法及び認証システムが得られる。

【０１２４】（第６の実施の形態）第６の実施形態の認証システムでは、認可サーバからクライアント手段に、認可通知とともに、利用回数が更新された認証チケットが送られる。

【０１２５】図１４は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図１４において図４と異なるのは、クライアント手段51及び認可サーバ手段53であって、認証サーバ手段32は変わりがない。また、認可サーバ53からクライアント手段51に、認可通知Result308とともに更新された認証チケットTicket501が送られる点が異なる。

【０１２６】この認証チケットTicket501は、認証チケット305に比べて、次の点が相違している。

【０１２７】即ち、認証チケット305でのｎ＋１段ハッシュ演算結果が、ｎ－ｋ＋１段ハッシュ演算結果（ｋは利用回数）に置き換えられている。認証チケット305での有効回数ｎが、残り利用可能回数ｎ－ｋに置き換えられている。タイムスタンプＴＳ０が新たなタイムスタンプＴＳｋに置き換えられている。発行者識別子ＩＩＤが認可サーバ53自身を示すサーバ識別子に置き換えられている。さらに、新たな認証子が付加されている。

【０１２８】この方法により、クライアント手段51は、パスワードＰＷを認可サーバ手段53を含めた第三者に明かすことなく、ｎ回まで認証チケット304や更新された認証チケット501を使用して利用認可を得ることができる。また、認証チケットのタイムスタンプが毎回更新されるため有効期限をより短く設定できる。そのため、不正な第三者による攻撃対象になりうる期間が短くなり、より安全性が高い。また、認可サーバ手段53におけるハッシュ演算が１段で良いため、利用認可手順における応答時間が短縮できる。

【０１２９】このようなプロトコルシーケンスを持つ認証システムの構成について図１５を参照しながら説明する。

【０１３０】図１５において、図５と異なるのは、クライアント手段51及び認可サーバ手段53であり、認証サーバ手段32は変わりがない。また、クライアント手段51において図５のクライアント手段31と異なるのは、チケット保持手段511が認可サーバ手段53からの認証チケットTicket501の認証チケットデータ5101も保持できるようにした点にある。また、認可サーバ手段53において図５の認可サーバ手段33と異なるのは、チケット利用管理手段531が残り利用可能回数をも出力するものとし、第３の多段ハッシュ手段336の代わりに１段のハッシュ演算Ｈを行なう第３のハッシュ手段532を設け、認証チケットに対する認証子を生成して付加する第２の認証子付加手段533を新たに設け、一部の結線を改めた点にある。

【０１３１】このチケット保持手段511としては、チケット保持手段314と同様の構成が結線を追加して使用できる。チケット利用管理手段531としては、チケット利用管理手段335と同様の構成が結線を追加して使用できる。第３のハッシュ手段532としては、例えばハッシュ演算Ｈのアルゴリズムを組み込んだ演算回路が使用できる。第２の認証子付加手段533としては、認証子付加手段328と同様の構成が使用できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【０１３２】以上のように構成された認証システムの動作について図１６を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数ｎをともなう場合について説明する。

【０１３３】まず、クライアント手段51及び認証サーバ手段32における動作は図５、図６の場合と同様で、ユーザ認証手順が行なわれて最終的には、認証サーバ手段32よりクライアント手段51へ認証チケットTicket304が送られる。

【０１３４】これに対してクライアント手段51においては、第１の送受信手段311は図５、図６の場合と同様に動作し、チケット保持手段511は図５、図６の場合のチケット保持手段314と同様に動作し、認証チケットTicket305が認可要求Authorize Requestとともに認可サーバ手段53に送られるとともに、認証チケットデータから有効回数3112が取出され多段ハッシュ手段317に送られる。

【０１３５】これに対して認可サーバ手段53においては、第３の送受信手段331、認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図５、図６の場合と同様に動作し、チケット識別子3305と多段ハッシュ値3306と有効回数3307と発行者識別子3308とチケット有効通知3310とをチケット利用管理手段531に供給する。チケット利用管理手段531は、図５、図６の場合のチケット利用管理手段335とほぼ同様に動作して、利用回数5301を第３の送受信手段331を介して認可チャレンジChallenge306としてクライアント手段51に送り、多段ハッシュ値3306をそのまま多段ハッシュ値5302として認可照合手段337に送るが、さらにチケット識別子と残り利用可能回数とサーバ識別子の組5303を出力して第２の認証子付加手段533に送る。

【０１３６】これに対するクライアント手段51の動作も図５、図６の場合と同様であり、認可チャレンジChallenge306に対して認可チャレンジ応答Response307が返される。

【０１３７】これに対して認可サーバ手段53においては、認可チャレンジ応答Response307は第３の送受信手段331で受信され、多段ハッシュ値5304が取出されて第３のハッシュ手段532及び第２の認証子付加手段533に送られる。第３のハッシュ手段532は、多段ハッシュ値5304にハッシュ演算Ｈを行なって、ハッシュの段数が１増えた二次多段ハッシュ値5305を認可照合手段337に送る（ＳＴ５３０１）。認可照合手段337は、多段ハッシュ値5302と二次多段ハッシュ値5305との一致判定を行ない（ＳＴ５３０２、ＳＴ３３１６）、照合結果5307を第２の認証子付加手段533に送る。

【０１３８】認可計時手段322は現在時刻を計時しており、現在時刻に基づくタイムスタンプ5306を第２の認証子付加手段533に供給している。第２の認証子付加手段533は、チケット識別子と残り利用可能回数とサーバ識別子の組5303と多段ハッシュ値5304とタイムスタンプ5306と認可サーバ53自身を示す発行者識別子とを連結し、これに対して認証子を生成して付加して認証チケットデータ5308とし（ＳＴ５３０３）、第３の送受信手段331を介して認証チケットTicket501として認可通知Result308とともにクライアント手段51に送る（ＳＴ５３０４）。

【０１３９】これに対してクライアント手段51においては、認証チケットTicket501は第１の送受信手段311で受信され、認証チケットデータ5101として前記チケット保持手段511に送られ保持されて（ＳＴ５１０１、ＳＴ５１０２）、次回の利用認可手順で使用される。

【０１４０】これによりクライアント手段51から認可サーバ手段53に送られる認証チケット305がともなう多段ハッシュ値は、その段数が利用認可ごとに１ずつ減って行くので、認可サーバ手段53ではハッシュ演算は１段のみ行なえば良く、応答時間が短縮できる。また、タイムスタンプが更新されるため有効期限をアクセスの間隔をカバーできる程度の短さ、例えば１時間に設定でき、ユーザ利便性は低下させずに安全性を高めることができる。この方法により、クライアント手段31はパスワードＰＷを認可サーバ手段53を含めた第三者に明かすことなく、安全性のより高い認証チケット305を使用してｎ回までより短い応答時間で利用認可を得ることができる。

【０１４１】なお、以上の説明ではクライアント手段51において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【０１４２】このように、本実施の形態の認証システムでは、第三者による不正使用の可能性をより小さくでき、また、利用認可の応答時間を短縮することができる。

【０１４３】（第７の実施の形態）第７の実施形態の認証システムは、認証チケットを複数の認可サーバに対して共通に用いることができる。

【０１４４】図１７は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図１７において図４と異なるのは、クライアント手段61、認証サーバ手段62、認可サーバ手段63であって、さらに認証チケット管理手段64を追加している。また、認証チャレンジ応答Response303を受けた認証サーバ手段62が認証要求Authenticate Request301から取出したチケット識別子ＴＩＤとサーバ識別子ＳＩＤと有効回数ｎとをともなった認証チケット発行登録指示Registration601を認証チケット管理手段64へ送る点、認可要求Authorize Request602が利用回数ｋをともなう点、認可要求Authorize Request602及び認証チケットTicket305を受けた認可サーバ手段6

3が認可要求Authorize Request602及び認証チケット305から取出したチケット識別子ＴＩＤとサーバ識別子ＳＩＤと利用回数ｋとをともなった認証チケット履歴更新指示Update603を認証チケット管理手段64へ送る点、これに対して必要に応じて認証チケット拒絶通知Reject606が返される点、認可チャレンジChallenge604が利用回数ｋの代わりに毎回異なるよう生成された乱数Ｒｋをともなう点、認可チャレンジ応答Response605がパスワードＰＷと乱数Ｒ０との連結に対してｎ－ｋ＋１段のハッシュ演算Ｈを施した結果にさらにＲｋとの排他的論理和演算を行なった結果をともなう点が異なる。

【０１４５】この方法により、クライアント手段61は、パスワードＰＷを認可サーバ手段63を含めた第三者に明かすことなく、ｎ回まで認証チケット304を使用して利用認可を得ることができ、利用回数ｋをクライアント手段61から送って認可サーバ手段63とは独立した認証チケット管理手段64でチェックするため、認証チケット304を複数の認可サーバ手段63で共通に利用可能とすることができる。

【０１４６】このプロトコルシーケンスを持つ認証システムの構成について図１８を参照しながら説明する。図１８においても図５と異なるのは、クライアント手段61、認証サーバ手段62、及び認可サーバ手段63であって、さらに認証チケット管理手段64を追加している。また、クライアント手段61において図５のクライアント手段31と異なるのは、認証チケットを保持するとともにその利用回数ｋを管理するチケット保持管理手段611をチケット保持手段314の代わりに設け、ビット毎の排他的論理和演算を行なう第１の排他的論理和手段612を設け、一部の結線を改めた点にある。また、認証サーバ手段62において図５の認証サーバ手段32と異なるのは、認証チケット発行登録指示データを生成するチケット登録指示手段621を設け、一部の結線を改めた点にある。

【０１４７】また、認可サーバ手段63において図５の認可サーバ手段33と異なるのは、認証チケットのチケット識別子と有効回数と残り利用可能回数を受取って各部に供給するとともに認証チケット履歴更新指示データを生成するチケット更新指示手段631をチケット利用管理手段335の代わりに設け、利用認可処理毎に乱数を生成する第２の乱数生成手段632、ビット毎の排他的論理和演算を行なう第２の排他的論理和手段633を設け、一部の結線を改めた点にある。

【０１４８】このチケット保持管理手段611としては、チケット保持手段335と同様の構成に利用回数の計算を行なう加算回路を追加して構成される。第１、第２の排他的論理和手段612、633としては、例えば論理回路が使用できる。チケット登録指示手段621としては、例えば論理回路が使用できる。チケット更新指示手段631としては、例えば論理回路が使用できる。第２の乱数生成手段632としては、乱数生成手段324と同様の構成が使用できる。認証チケット管理手段64としては、各種通信インタフェース装置とデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【０１４９】以上のように構成された認証システムの動作について図１９を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数ｎをともなう場合について説明する。

【０１５０】まず、ユーザ認証手順におけるクライアント手段61及び認証サーバ手段62における動作は図５、図６の場合とほぼ同様で、最終的には認証サーバ手段62よりクライアント手段61へ認証チケットTicket304が送られる。ただし、クライアント手段61においては、このときのチケット保持手段314の動作をチケット保持管理手段611が行なう。また認証サーバ手段62においては、認証要求Authenticate Request301から取出された有効回数6201は多段ハッシュ手段325及び認証子付加手段328のほかチケット登録指示手段621にも送られ、サーバ識別子6202は認証子付加手段328のほかチケット登録指示手段621にも送られ、チケット識別子生成手段327で生成されたチケット識別子6203は認証子付加手段328のほかチケット登録指示手段621にも送られる。

【０１５１】チケット登録指示手段621は、チケット識別子6203とサーバ識別子6202と有効回数6201とを連結して認証チケット発行登録指示データ6204を生成し、第２の送受信手段321を介して認証チケット発行登録指示Registration601として認証チケット管理手段64に送る（ＳＴ６２０１）。これを受けた認証チケット管理手段64はチケットリストを管理しており、認証チケット発行登録指示Registration601が与えられた場合に、チケット識別子を用いてチケットリスト中を検索して既に登録されているかを調べる。該当するものが無ければチケット識別子と有効回数と残り利用可能回数を示す値としての有効回数の組をチケットリストに追加し記憶する。

【０１５２】これに対してクライアント手段61においては、認証チケットTicket304は第１の送受信手段311で受信され、認証チケットデータ3110が取出されてチケット保持管理手段611に送られる。チケット保持管理手段611は認証チケットデータ3110をサーバ識別子3101と対応づけて保持し、認証チケットデータから取出した有効回数を残り利用可能回数として同時に管理し（ＳＴ６１０１）、利用認可手順起動通知6101が与えられた場合に、認証チケットデータ3111を第１の送受信手段311を介して認証チケットTicket305として、また、残り利用可能

回数を１減じたうえで認証チケットから取出した有効回数から引くことにより得た利用回数6102を（ＳＴ６１０２）第１の送受信手段311を介して認可要求Authorize Request602として、認可サーバ手段63に送り（ＳＴ６１０３）、さらに、認証チケットデータから取出した有効回数3112を多段ハッシュ手段317に送る。

【０１５３】これに対して認可サーバ手段63においては、認証チケットTicket305及び認可要求Authorize Request602は第３の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られ、利用回数6301が取出されてチケット更新指示手段631に送られる（ＳＴ６３０１）。認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図５、図６の場合とほぼ同様に動作し、ただし、サーバ識別子6302はチケット有効判定手段334のほかチケット更新指示手段631にも送られ、有効通知6303はチケット更新指示手段631及び第２の乱数生成手段632に送られる。チケット更新指示手段631は、有効通知6303が与えられると、チケット識別子3305とサーバ識別子6302と利用回数6301とを連結して認証チケット履歴更新指示データ6304を生成し、第３の送受信手段331を介して認証チケット履歴更新指示Update603として認証チケット管理手段64に送る（ＳＴ６３０２）とともに、利用回数6301をそのまま利用回数6306として第３の多段ハッシュ手段336へ送る。認証チケット管理手段64は、認証チケット履歴更新指示Update603が与えられた場合に、チケット識別子を用いてチケットリスト中を検索し、対応する有効回数を示す値が、対応する残り利用可能回数を示す値と認証チケット履歴更新指示Update603がともなう利用回数との合計に一致することをチェックして、正しければチケットリスト中の残り利用可能回数を示す値を１減じ、正しくなければ認証チケット拒絶通知Reject606を送り返す。認証チケット拒絶通知606は認可サーバ手段63において、第３の送受信手段331を介して認証チケット拒絶通知データ6305として前記チケット更新指示手段631に送られる。チケット更新指示手段631は、多段ハッシュ値3306をそのまま多段ハッシュ値3312として認可照合手段337に送るが、認証チケット拒絶通知データ6305が与えられるとこれを抑止する。第２の乱数生成手段632は、有効通知6303が与えられると、データ撹乱用のチャレンジ乱数6307を新たにランダムに生成して第２の排他的論理和手段633に送るとともに、第３の送受信手段331を介して認可チャレンジChallenge604としてクライアント手段61に送る（ＳＴ６３０３）。

【０１５４】これに対してクライアント手段61においては、認可チャレンジChallenge604は第１の送受信手段311で受信され、チャレンジ乱数6103が取出されて第１の排他的論理和手段612に送られる（ＳＴ６１０４）。多段ハッシュ手段317は、利用認可手順起動通知6101が与えられている場合に、前記機密記憶手段316よりハッシュ値3113を得て、ハッシュ値3113に有効回数3112と利用回数6102との差に相当する段数のハッシュ演算Ｈを行なって、結果の多段ハッシュ値6104を、第１の排他的論理和手段612に送る。第１の排他的論理和手段612は、利用認可手順起動通知6101が与えられている場合に、多段ハッシュ値6104とチャレンジ乱数6103との間でビット毎の排他的論理和演算を行ない、撹乱多段ハッシュ値6105を生成し、第１の送受信手段311を介して認可チャレンジ応答Response605として認可サーバ手段63に送る（ＳＴ６１０５、ＳＴ６１０６）。ハッシュ演算Ｈが充分安全な一方向性と結果の長さ及びランダム性を持っている限り、この撹乱多段ハッシュ値6105はパスワードＰＷ、乱数Ｒ０及びチャレンジ乱数を知らない第三者には計算することができないため、この撹乱多段ハッシュ値6105によりパスワードＰＷを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Ｈの段数が多く行なわれているため、この多段ハッシュ値6104から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも１００倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【０１５５】これに対して認可サーバ手段63においては、認可チャレンジ応答Response605は第３の送受信手段331で受信され、撹乱多段ハッシュ値6308が取出されて第２の排他的論理和手段633に送られる（ＳＴ６３０４）。第２の排他的論理和手段633は、チャレンジ乱数6307と撹乱多段ハッシュ値6308との間でビット毎の排他的論理和演算を行なって、多段ハッシュ値6309を得て第３の多段ハッシュ手段336に送る（ＳＴ６３０５）。第３の多段ハッシュ手段336は、多段ハッシュ値6309に利用回数6306に相当する段数のハッシュ演算を行なって、結果の二次多段ハッシュ値3314を認可照合手段337に送る。認可照合手段337は図５、図６の場合と同様に動作し、認可通知データ3315を第３の送受信手段331を介して認可通知Result308としてクライアント手段61に送り、クライアント手段61において受信される。ただし、認証チケット拒絶通知Reject606の受信により多段ハッシュ値3312の供給が抑止された場合にはこの限りではない（ＳＴ６３０６，ＳＴ６３０７）。この方法により、クライアント手段61はパスワードＰＷを認可サーバ手段63を含めた第三者に明かすことなく、ｎ回まで認証チケット305を使用して複数の認可サーバ手段に対して利用認可を得ることができる。

【０１５６】なお、以上の説明ではクライアント手段61において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる

必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【０１５７】このように、この実施形態では、認証チケットが更新されない方式の下で、認証チケットを複数の認可サーバに対して共通に用いることができる、利便性の高いシングルサインオン型の認証システムを構成することができる。

【０１５８】（第８の実施の形態）第８の実施形態の認証システムは、認証チケットの利用を分散管理することができる。

【０１５９】図２０は、この認証システムのプロトコルを示すプロトコルシーケンス図である。図２０において図１４と異なるのは、クライアント手段71、認証サーバ手段72及び認可サーバ手段73であって、さらに第２の認可サーバ手段74を追加している。また、認可要求Authorize Request701が利用回数ｋをともなう点、認可要求Authorize Request701及び認証チケットTicket305を受けた認可サーバ手段73が認可要求Authorize Request701及び認証チケット305から取出したチケット識別子ＴＩＤとサーバ識別子ＳＩＤと利用回数ｋとをともなった認証チケット履歴照会Inquiry702を認証サーバ手段72または第２の認可サーバ手段74へ送る点、これに対して必要に応じて認証チケット拒絶通知Reject705が返される点、認可チャレンジChallenge703が利用回数ｋの代わりに毎回異なるよう生成された乱数Ｒｋをともなう点、認可チャレンジ応答Response704がパスワードＰＷと乱数Ｒ０との連結に対してｎ－ｋ＋１段のハッシュ演算Ｈを施した結果にさらにＲｋとの排他的論理和演算を行なった結果をともなう点が異なる。

【０１６０】この方法により、クライアント手段71はパスワードＰＷを認可サーバ手段73、第２の認可サーバ手段74を含めた第三者に明かすことなく、ｎ回まで認証チケット304や更新された認証チケット501を使用して利用認可を得ることができ、利用回数ｋをクライアント手段71から認可サーバ手段73を介して認証チケットを発行した認証サーバ手段72または更新した第２の認可サーバ手段74に送ってチェックするため、認証チケット304を複数の認可サーバ手段73、74で共通に利用可能なものとすることができ、かつチェック処理のトラフィックを分散化できる。

【０１６１】このようなプロトコルシーケンスを持つ認証システムの構成について図２１を参照しながら説明する。図２１においても図１５と異なるのは、クライアント手段71、認証サーバ手段72、認可サーバ手段73であって、さらに第２の認可サーバ手段74を追加している。また、クライアント手段71において図１５のクライアント手段51と異なるのは、認証チケットを保持するとともにその利用回数ｋを管理するチケット保持管理手段711をチケット保持手段511の代わりに設け、ビット毎の排他的論理和演算を行なう第１の排他的論理和手段712を設け、一部の結線を改めた点にある。また、認証サーバ手段72において図１５の認証サーバ手段32と異なるのは、認証チケットの発行を管理して照会に回答するチケット発行管理手段721を設け、一部の結線を改めた点にある。また、認可サーバ手段73において図１５の認可サーバ手段53と異なるのは、認証チケットのチケット識別子と有効回数と残り利用可能回数とを受取って各部に供給するとともに認証チケットの更新を管理して照会に回答するチケット更新管理手段731をチケット利用管理手段531の代わりに設け、利用認可処理毎に乱数を生成する第２の乱数生成手段732、ビット毎の排他的論理和演算を行なう第２の排他的論理和手段733を設け、一部の結線を改めた点にある。第２の認可サーバ手段74は認可サーバ手段73と同様の構成を持つものである。

【０１６２】チケット保持管理手段711としては、チケット保持手段511と同様の構成に利用回数の計算を行なう加算回路を追加して使用できる。第１、第２の排他的論理和手段712、733としては、例えば論理回路が使用できる。チケット発行管理手段721としては、例えばデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。チケット更新管理手段731としては、例えばデータの分割結合を行なう論理回路と利用回数を照合する演算回路及び比較回路と大容量のメモリデバイスとの組合せにより構成できる。第２の乱数生成手段732としては、乱数生成手段324と同様の構成が使用できる。なお、上記各手段をマイクロコンピュータまたは汎用コンピュータ上のコンピュータプログラムを使用して実現しても良い。あるいはそのコンピュータプログラムを読取り可能な形式でプログラム記録媒体に記録し、プログラム記録媒体読取り装置と組み合わせた構成により実現しても良い。

【０１６３】以上のように構成された認証システムの動作について図２２を参照しながら説明する。ここでは、認証要求Authenticate Request301が認証チケット有効回数ｎをともなう場合について説明する。

【０１６４】まず、ユーザ認証手順におけるクライアント手段71及び認証サーバ手段72における動作は図１５、図１６の場合とほぼ同様で、最終的には認証サーバ手段72よりクライアント手段71へ認証チケットTicket304が送られる。ただし、クライアント手段71においては、このときのチケット保持手段511の動作をチケット保持管理手段711が行なう。また認証サーバ手段72においては、認証要求Authenticate Request301から取出された有効回数7201は多段ハッシュ手段325及び認証子付加手段328のほかチケット発行管理手段721にも送られ、サーバ識別子7202は認証子付加手段328のほかチケット発行管理手段721にも送られ、チケット識別子生成手段327で生成されたチケット識別子7203は認証子付加手段328のほかチケット発行管理手段721にも送られる。チケット

発行管理手段721は発行したチケットリストを管理しており、チケット識別子7203とサーバ識別子7202と有効回数7201と残り利用可能回数を示す値としての有効回数7201の組をチケットリストに追加し記憶する（ＳＴ７２０１）。

【０１６５】これに対してクライアント手段71においては、認証チケットTicket304は第１の送受信手段311で受信され、認証チケットデータ3110が取出されて前記チケット保持管理手段711に送られる。前記チケット保持管理手段711は、認証チケットデータ3110をサーバ識別子3101と対応づけて保持し、認証チケットデータから取出した有効回数を残り利用可能回数として同時に管理し（ＳＴ７１０１）、利用認可手順起動通知7101が与えられた場合に、認証チケットデータ3111を第１の送受信手段311を介して認証チケットTicket305として、また、残り利用可能回数を１減じたうえで認証チケットから取出した有効回数から引くことにより得た利用回数7102を（ＳＴ７１０２）第１の送受信手段311を介して認可要求Authorize Request701として、それぞれ認可サーバ手段73に送り（ＳＴ７１０３）、さらに認証チケットデータから取出した有効回数3112を多段ハッシュ手段317に送る。

【０１６６】これに対して認可サーバ手段73においては、認証チケットTicket305及び認可要求Authorize Request701は第３の送受信手段331で受信され、認証チケットデータ3301が取出されて認証子検証手段333に送られ、利用回数7301が取出されてチケット更新管理手段731に送られる（ＳＴ７３０１）。

【０１６７】認可計時手段332、認証子検証手段333及びチケット有効判定手段334は図１５、図１６の場合とほぼ同様に動作し、ただし、サーバ識別子7302はチケット有効判定手段334のほかチケット更新管理手段731にも送られ、有効通知7303はチケット更新管理手段731及び第２の乱数生成手段732に送られる。チケット更新管理手段731は発行したチケットリストを管理しており、有効通知7303が与えられると、チケット識別子3305とサーバ識別子7302と利用回数7301とを連結して認証チケット履歴照会データ7304を得て、第３の送受信手段331を介して発行者識別子3308の示す認証サーバ手段72または第２の認可サーバ手段74へ認証チケット履歴照会Inquiry702を送るとともに、チケット識別子3305とサーバ識別子7302と有効回数7301と残り利用可能回数を示す値としての有効回数7301の組をチケットリストに追加し記憶する（ＳＴ７３０２）。

【０１６８】これを受けた認証サーバ手段72では、認証チケット履歴照会Inquiry702は第２の送受信手段321で受信され、チケット識別子とサーバ識別子と利用回数とを含んだ認証チケット履歴照会データ7205として前記チケット発行管理手段721に送られる。前記チケット発行管理手段721は、認証チケット履歴照会データ7205から取出した利用回数が、自ら管理する有効回数と残り利用可能回数との差に１加えたものと一致するかを調べ、不一致の場合には認証チケット拒絶通知データ7204を第２の送受信手段321を介して認証チケット拒絶通知Reject705として送り返す。なお、第２の認可サーバ手段74がこれを受けた場合には、チケット更新管理手段が前記チケット発行管理手段721と同様の役割を行なう。

【０１６９】認可サーバ手段73においては、認証チケット拒絶通知705は第３の送受信手段331を介して認証チケット拒絶通知データ7305として前記チケット更新管理手段731に送られる。前記チケット更新管理手段731は、多段ハッシュ値3306をそのまま多段ハッシュ値5302として認可照合手段337に送り、チケット識別子と残り利用可能回数とサーバ識別子との組5303を第２の認証子付加手段533に送るが、認証チケット拒絶通知データ7305が与えられるとこれらを抑止する。第２の乱数生成手段732は、有効通知7303が与えられると、データ撹乱用のチャレンジ乱数7306を新たにランダムに生成して第２の排他的論理和手段733に送るとともに、第３の送受信手段331を介して認可チャレンジChallenge703としてクライアント手段71に送る（ＳＴ７３０３）。

【０１７０】これに対してクライアント手段71においては、認可チャレンジChallenge703は第１の送受信手段311で受信され、チャレンジ乱数7103が取出されて第１の排他的論理和手段712に送られる（ＳＴ７１０４）。多段ハッシュ手段317は、利用認可手順起動通知7101が与えられている場合に、前記機密記憶手段316よりハッシュ値3113を得て、ハッシュ値3113に有効回数3112と利用回数7102との差に相当する段数のハッシュ演算Ｈを行なって、結果の多段ハッシュ値7104を、第１の排他的論理和手段712に送る。第１の排他的論理和手段712は、利用認可手順起動通知7101が与えられている場合に、多段ハッシュ値7104とチャレンジ乱数7103との間でビット毎の排他的論理和演算を行ない、撹乱多段ハッシュ値7105を生成し、第１の送受信手段311を介して認可チャレンジ応答Response704として認可サーバ手段73に送る（ＳＴ７１０５、ＳＴ７１０６）。ハッシュ演算Ｈが充分安全な一方向性と結果の長さ及びランダム性を持っている限り、この撹乱多段ハッシュ値7105はパスワードＰＷ、乱数Ｒ０及びチャレンジ乱数を知らない第三者には計算することができないため、この撹乱多段ハッシュ値7105によりパスワードＰＷを知る正当なユーザであることが示される。また、過去にさかのぼるほど多段ハッシュ値におけるハッシュ演算Ｈの段数が多く行なわれているため、この多段ハッシュ値7104から次の多段ハッシュ値を計算することもできないので、暗号化の必要もない。なお、ハッシュ演算は一般に暗号演算よりも１００倍以上高速であるとされ、適切な段数であれば暗号を用いた場合よりも高速に処理が行なえる。

【０１７１】これに対して認可サーバ手段73において

は、認可チャレンジ応答Response704は第３の送受信手段331で受信され、撹乱多段ハッシュ値7307が取出されて第２の排他的論理和手段733に送られる（ＳＴ７３０４）。第２の排他的論理和手段733は、チャレンジ乱数7306と撹乱多段ハッシュ値7307との間でビット毎の排他的論理和演算を行なって、多段ハッシュ値7308を得て第３のハッシュ手段532に送る（ＳＴ７３０５）。第３のハッシュ手段532は、多段ハッシュ値7308にハッシュ演算を行なって、結果の二次多段ハッシュ値5305を認可照合手段337に送る。認可照合手段337及び第２の認証子付加手段533は図１５、図１６の場合と同様に動作し、認証チケットデータ5308を第３の送受信手段331を介して認証チケットTicket501としてクライアント手段71に送る。ただし、認証チケット拒絶通知Reject705の受信により多段ハッシュ値5302及びチケット識別子と残り利用可能回数とサーバ識別子との組5303の供給が抑止された場合にはこの限りではない（ＳＴ７３０６，ＳＴ７３０７）。

【０１７２】これに対してクライアント手段71においては、認証チケットTicket501は第１の送受信手段311で受信され、認証チケットデータ5101として前記チケット保持管理手段711に送られ保持されて（ＳＴ７１０７、ＳＴ７１０８）、次回の利用認可手順で使用される。

【０１７３】これによりクライアント手段71から認可サーバ手段73に送られる認証チケット305がともなう撹乱多段ハッシュ値は、その段数が利用認可ごとに１ずつ減って行くので、認可サーバ手段73ではハッシュ演算は１段のみ行なえば良く、応答時間が短縮できる。また、タイムスタンプが更新されるため有効期限をアクセスの間隔をカバーできる程度の短さ、例えば１時間に設定でき、ユーザ利便性は低下させずに安全性を高めることができる。この方法により、クライアント手段71はパスワードＰＷを認可サーバ手段73、74を含めた第三者に明かすことなく、安全性のより高い認証チケット305を使用してｎ回まで、より短い応答時間で利用認可を得ることができ、その認証チケットは複数の認可サーバで共通に利用可能で、かつチェック処理のトラフィックを分散化できる。

【０１７４】なお、以上の説明ではクライアント手段71において利用認可手順のたびに多段ハッシュ値を計算する構成としたが、認証チケットの取得時にすべての段数の多段ハッシュ値を事前計算して機密記憶手段316に記憶する構成としても良い。その場合、機密記憶手段316としてより大容量の耐タンパ性メモリデバイスを用いる必要があるものの、利用認可手順ごとの処理時間をより短くすることができる。

【０１７５】このように、認証システムを本実施形態のように構成することにより、認証チケットが更新される方式の下で、認証チケットの利用を分散管理することができる。そのため１個所の管理リソースをより少なくできる。

【０１７６】

【発明の効果】以上の説明から明らかなように、本発明では、第１に、クライアント側での暗号処理を必要とせず、認証チケットの使用回数を容易に管理して二重使用を排除することができる、シングルサインオン型の認証方法及び認証システムが得られる。

【０１７７】第２に、ユーザ認証手順においても、クライアント側での暗号処理を必要としないうえ、認証提示情報の演算処理と提示情報の演算処理とが共通化できる、シングルサインオン型の認証方法及び認証システムが得られる。

【０１７８】第３に、クライアント手段が生成した認証用乱数を秘密情報として照合情報を生成するものでは、認証チケットが含む照合情報がユーザ認証情報と無関係となるため認証チケットからユーザ認証情報が推測される可能性すらなく、より安全性の高いシングルサインオン型の認証方法及び認証システムが得られる。

【０１７９】第４に、秘密情報の不可逆演算を一方向性ハッシュ演算で行なうことにより、クライアント側が計算処理能力の低い装置であっても実用的な処理時間で利用認可処理を行なうことができる、シングルサインオン型の認証方法及び認証システムが得られる。

【０１８０】第５に、認可サーバ手段が認証チケットの照合情報等を更新するものでは、認証チケットが使用するごとに更新され、特にタイムスタンプが更新されるため有効判定における有効期限をより短く設定できるので、第三者による不正使用の可能性をより小さくでき、さらに利用認可の応答時間を短縮できる、シングルサインオン型の認証方法及び認証システムが得られる。

【０１８１】第６に、認証チケットの使用回数を管理する認証チケット管理手段を設けたものでは、認証チケットが更新されないシステムにおいて、認証チケットを複数の認可サーバに対して共通に用いることが可能となるため、より利便性の高いシングルサインオン型の認証方法及び認証システムが得られる。

【０１８２】第７に、認証サーバ手段や認可サーバ手段が認証チケットの発行履歴を記憶するものでは、認証チケットが更新されるシステムにおいて、認証チケットの利用を分散管理できるため１個所の管理リソースをより少なくできる、シングルサインオン型の認証方法及び認証システムが得られる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態における認証システムの概要を示す概念図、

【図２】本発明の第２の実施の形態における認証システムの概要を示す概念図、

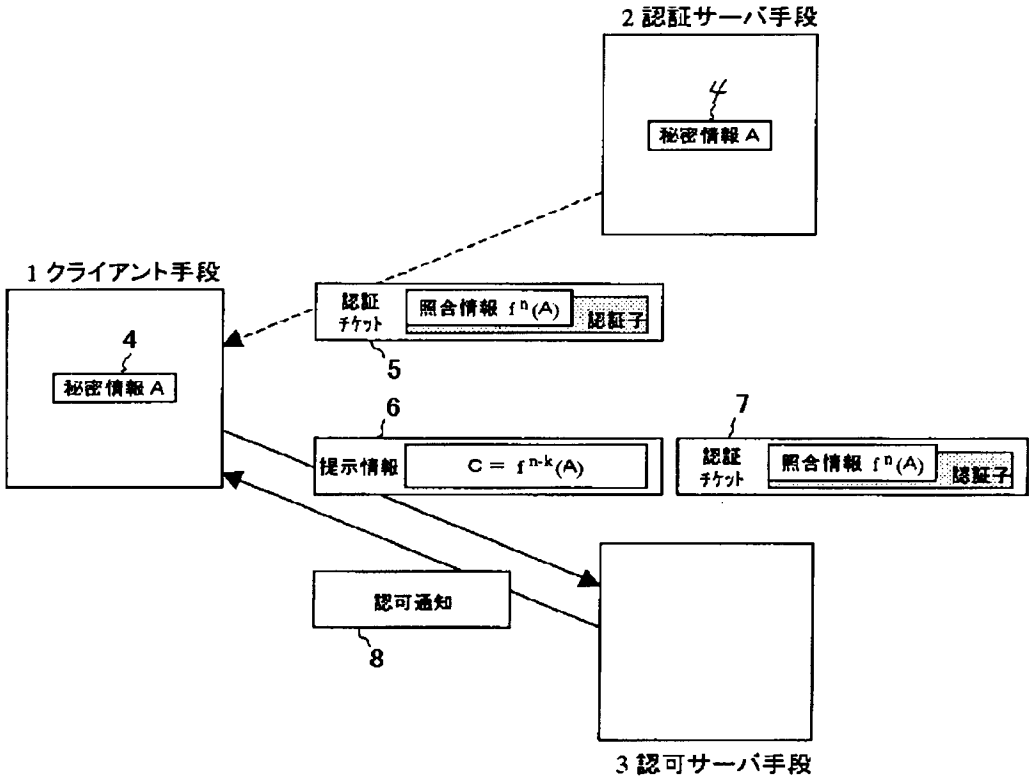
【図３】本発明の第３の実施の形態における認証システムの概要を示す概念図、

【図４】本発明の第４の実施の形態における認証システ

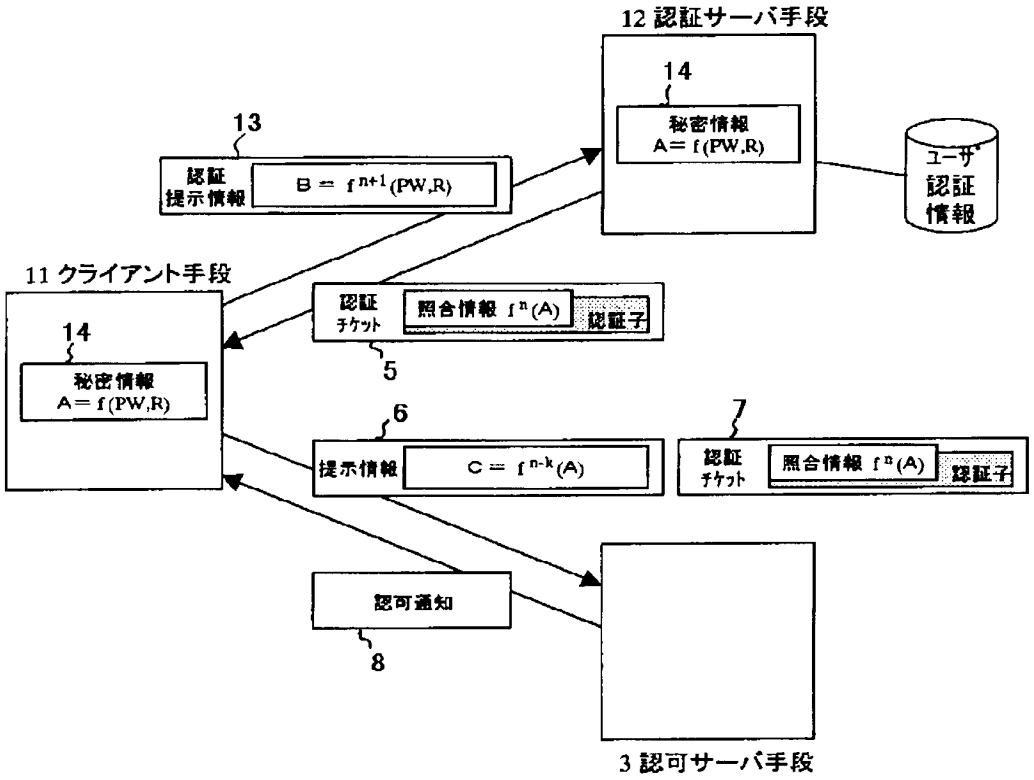
ムのプロトコルシーケンス図、
【図５】本発明の第４の実施の形態における認証システムの機能ブロック図、
【図６】本発明の第４の実施の形態における認証システムの動作を示すフロー図、
【図７】本発明の第４の実施の形態における認証システムにおいてメッセージ認証コードを用いた場合の認証子付加手段の詳細な機能ブロック図、
【図８】本発明の第４の実施の形態における認証システムにおいてメッセージ認証コードを用いた場合の認証子検証手段の詳細な機能ブロック図、
【図９】本発明の第４の実施の形態における認証システムにおいてデジタル署名を用いた場合の認証子付加手段の詳細な機能ブロック図、
【図１０】本発明の第４の実施の形態における認証システムにおいてデジタル署名を用いた場合の認証子検証手段の詳細な機能ブロック図、
【図１１】本発明の第５の実施の形態における認証システムのプロトコルシーケンス図、
【図１２】本発明の第５の実施の形態における認証システムの機能ブロック図、
【図１３】本発明の第５の実施の形態における認証システムの動作を示すフロー図、
【図１４】本発明の第６の実施の形態における認証システムのプロトコルシーケンス図、
【図１５】本発明の第６の実施の形態における認証システムの機能ブロック図、
【図１６】本発明の第６の実施の形態における認証システムの動作を示すフロー図、
【図１７】本発明の第７の実施の形態における認証システムのプロトコルシーケンス図、
【図１８】本発明の第７の実施の形態における認証システムの機能ブロック図、
【図１９】本発明の第７の実施の形態における認証システムの動作を示すフロー図、
【図２０】本発明の第８の実施の形態における認証システムのプロトコルシーケンス図、
【図２１】本発明の第８の実施の形態における認証システムの機能ブロック図、
【図２２】本発明の第８の実施の形態における認証システムの動作を示すフロー図、
【図２３】従来の認証方法の概要を示す概念図、
【図２４】従来の認証方法のプロトコルシーケンス図、
【図２５】従来の認証方法の機能ブロック図、
【図２６】従来の認証方法の動作を示すフロー図である。
【符号の説明】
１、11、21、31、41、51、61、71、81　クライアント手段
２、12、22、32、42、62、72、82　認証サーバ手段
３、33、53、63、73、83　認可サーバ手段
４、14、24　秘密情報
５、７、803、805　認証チケット
６、804　提示情報
８、806　認可通知
13、23、801　認証提示情報
64　認証チケット管理手段
74　第２の認可サーバ手段
311　第１の送受信手段
312、811　入力手段
313　ハッシュ手段
314　チケット保持手段
316　機密記憶手段
317　多段ハッシュ手段
321　第２の送受信手段
322　認証計時手段
323　認証情報蓄積手段
324　乱数生成手段
325　第２の多段ハッシュ手段
326　認証照合手段
327　チケット識別子生成手段
328　認証子付加手段
328A　自識別子記憶手段
328B　データ連結手段
328C　連結データハッシュ手段
328D　サーバ共通鍵記憶手段
328E　共通鍵方式暗号手段
328F　認証子連結手段
328G　自秘密鍵記憶手段
328H　公開鍵方式暗号手段
331　第３の送受信手段
332　認可計時手段
333　認証子検証手段
333A　認証子分離手段
333B　第２の連結データハッシュ手段
333C　第２のサーバ共通鍵記憶手段
333D　第２の共通鍵方式暗号手段
333E　データ分離手段
333F　発行者識別子照合手段
333G　比較手段
333H　サーバ公開鍵蓄積手段
333J　公開鍵方式復号手段
334、832　チケット有効判定手段
335、531　チケット利用管理手段
336　第３の多段ハッシュ手段
337　認可照合手段
411　認証用乱数生成手段
412、612、712　第１の排他的論理和手段
421　第２のハッシュ手段
422　第２の排他的論理和手段

423　第２の多段ハッシュ手段
511　チケット保持手段
532　第３のハッシュ手段
533　第２の認証子付加手段
611、711　チケット保持管理手段
621　チケット登録指示手段
631　チケット更新指示手段
632　第２の乱数生成手段
633、733　第２の排他的論理和手段
721　チケット発行管理手段
731　チケット更新管理手段
732　第２の乱数生成手段
812　セッション鍵復号手段
813　証明計時手段
814　証明情報暗号手段
821　セッション鍵生成手段
822　セッション鍵暗号手段
823　チケット暗号手段
831　チケット復号手段
833　証明情報復号手段
834　証明情報有効判定手段
835　認可照合手段

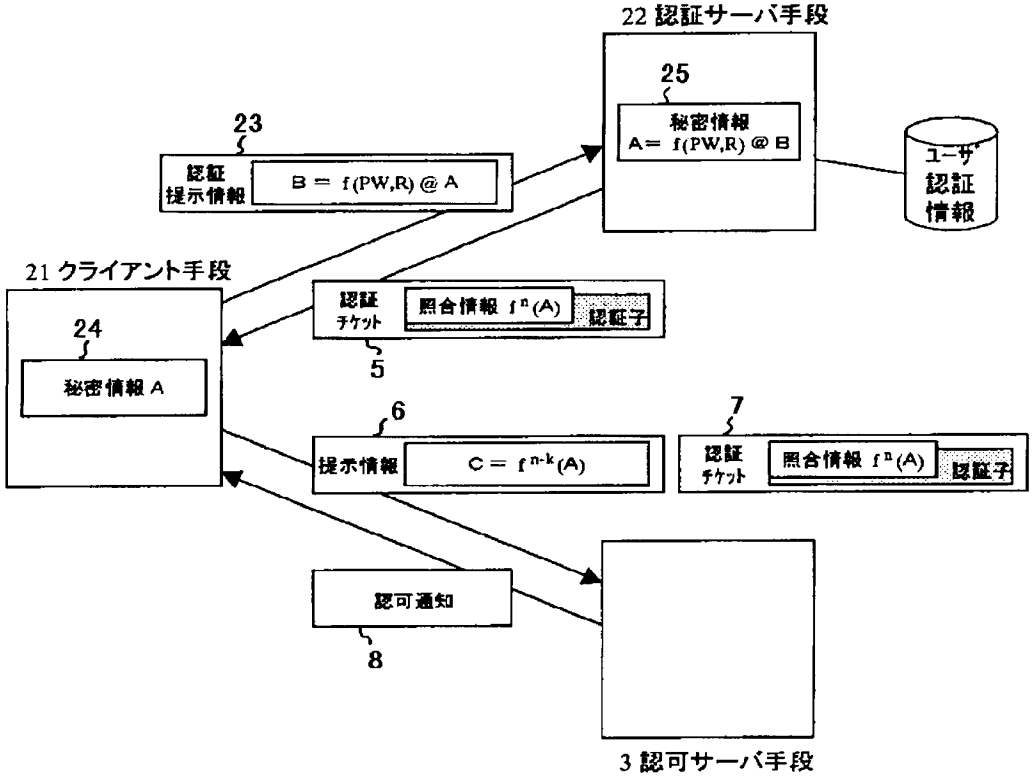
【図１】



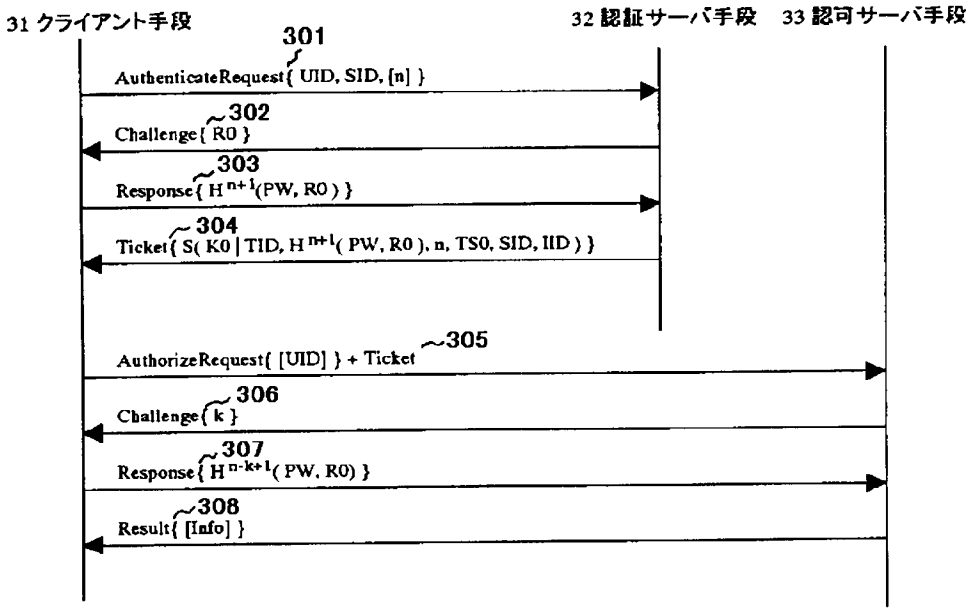
【図２】


12 認証サーバ手段
14
秘密情報
A＝ f(PW,R)
13
認証
提示情報
B ＝ f n+1(PW,R)
ユーザ
認証
情報
11 クライアント手段
認証
チケット
照合情報 f n(A)
認証子
5
14
秘密情報
A＝ f(PW,R)
6
提示情報
C ＝ f n-k(A)
7
認証
チケット
照合情報 f n(A)
認証子
認可通知
8
3 認可サーバ手段

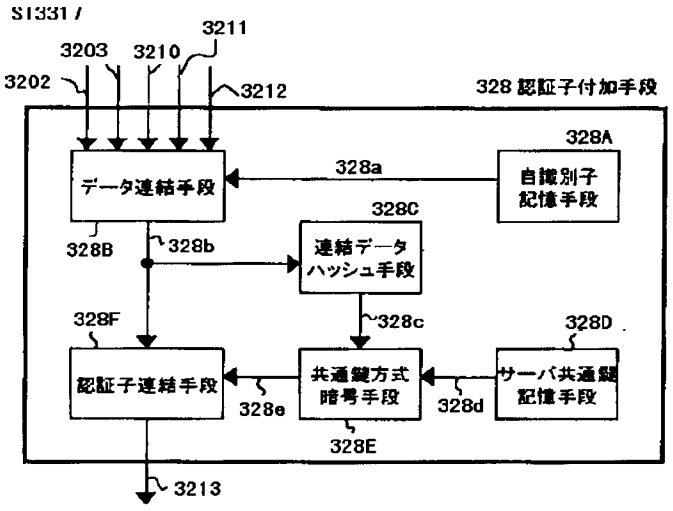
【図３】


22 認証サーバ手段
25
秘密情報
A＝ f(PW,R) @ B
23
認証
提示情報
B ＝ f(PW,R) @ A
ユーザ
認証
情報
21 クライアント手段
認証
チケット
照合情報 f n(A)
認証子
5
24
秘密情報 A
6
提示情報
C ＝ f n-k(A)
7
認証
チケット
照合情報 f n(A)
認証子
認可通知
8
3 認可サーバ手段

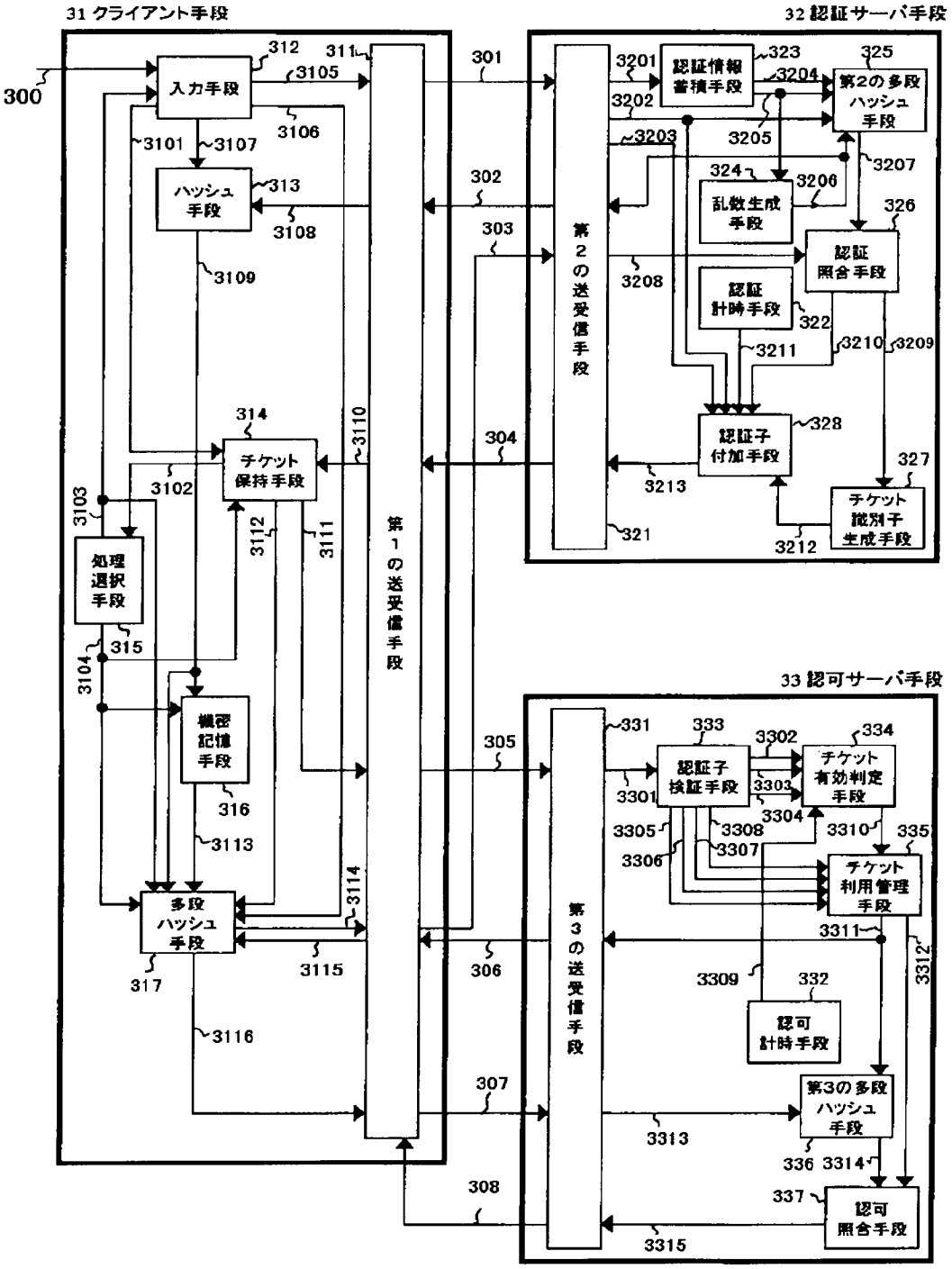
【図４】


31 クライアント手段
32 認証サーバ手段
33 認可サーバ手段
301
AuthenticateRequest{ UID, SID, [n] }
302
Challenge{ R0 }
303
Response{ H^{n+1}(PW, R0) }
304
Ticket{ S(K0 | TID, H^{n+1}(PW, R0), n, TS0, SID, IID) }
305
AuthorizeRequest{ [UID] } + Ticket
306
Challenge{ k }
307
Response{ H^{n-k+1}(PW, R0) }
308
Result{ [Info] }

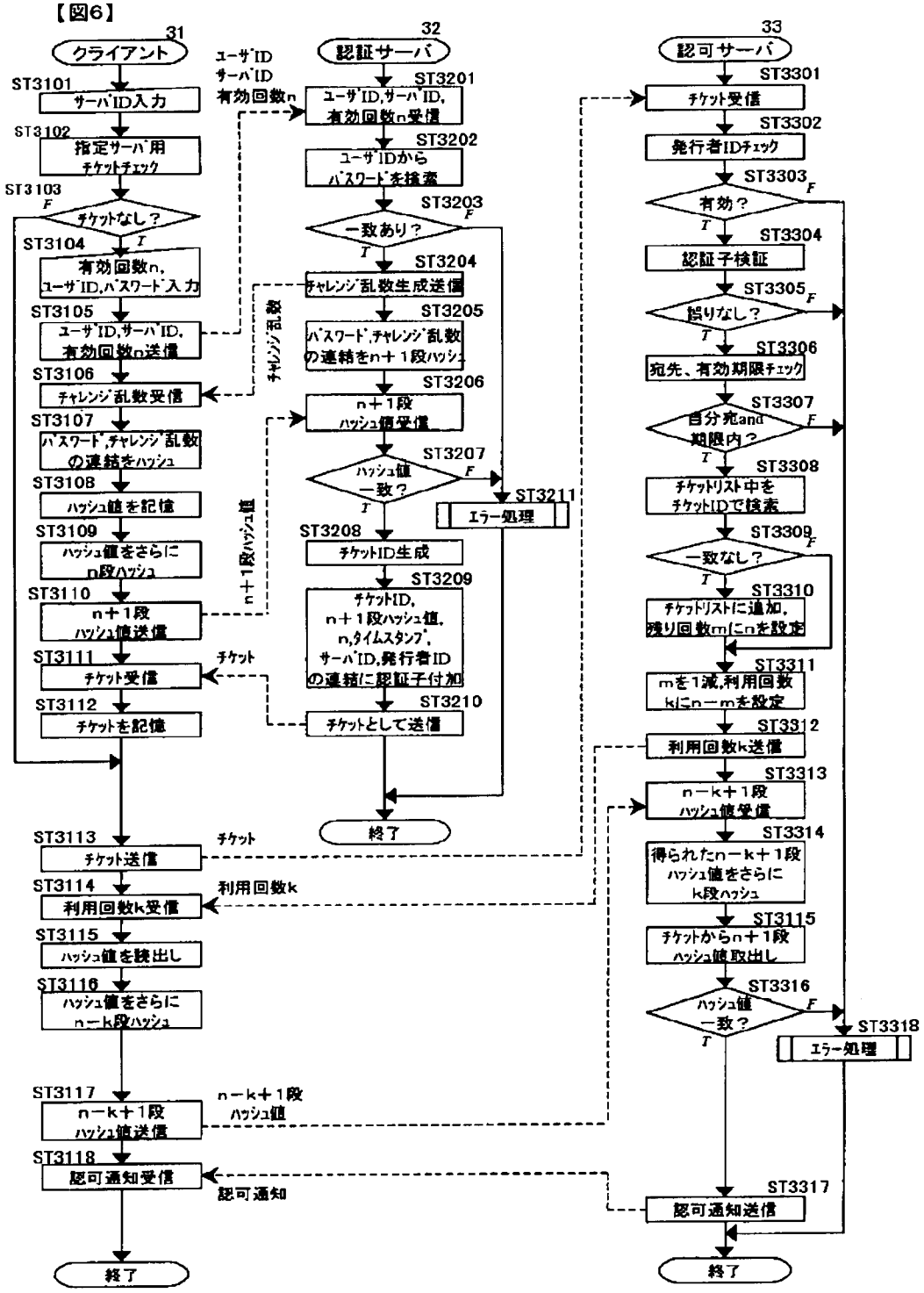
【図７】


S1331 /
3211
3203
3210
3202
3212
328 認証子付加手段
328A
データ連結手段
328a
自識別子記憶手段
328C
328B
328b
連結データハッシュ手段
328F
328c
328D
認証子連結手段
328e
共通鍵方式暗号手段
328d
サーバ共通鍵記憶手段
328E
3213

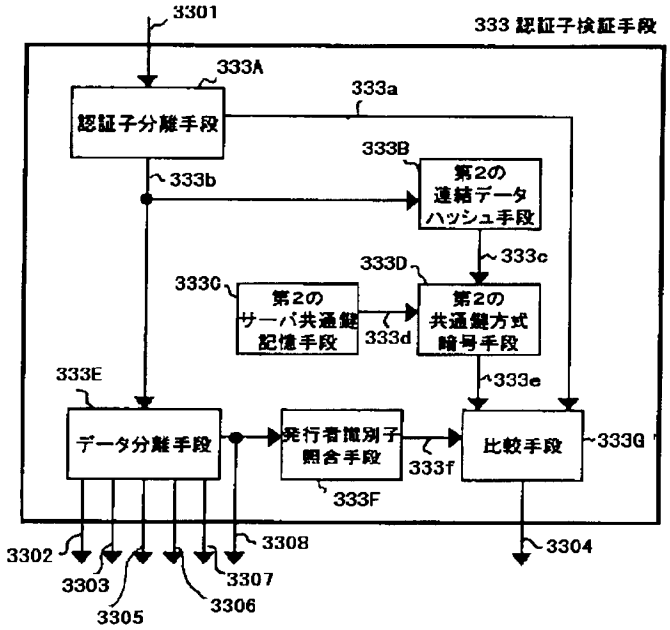
【図５】


31 クライアント手段
32 認証サーバ手段
33 認可サーバ手段
300
入力手段
312
311
3105
3106
3101
3107
ハッシュ手段
313
3108
3109
チケット保持手段
314
3110
3102
3103
処理選択手段
315
3104
機密記憶手段
316
3113
多段ハッシュ手段
3114
3115
317
3116
3112
3111
第一の送受信手段
301
302
303
304
305
306
307
308
第２の送受信手段
3201
認証情報蓄積手段
323
3204
第2の多段ハッシュ手段
325
3202
3205
3203
3207
324
乱数生成手段
3206
326
認証照合手段
3208
認証計時手段
322
3211
3210
3209
認証子付加手段
328
3213
327
チケット識別子生成手段
3212
321
第３の送受信手段
331
333
3302
334
認証子検証手段
3301
3303
チケット有効判定手段
3304
3305
3308
3310
335
3306
3307
チケット利用管理手段
3311
3312
3309
332
認可計時手段
第3の多段ハッシュ手段
3313
336
3314
337
認可照合手段
3315

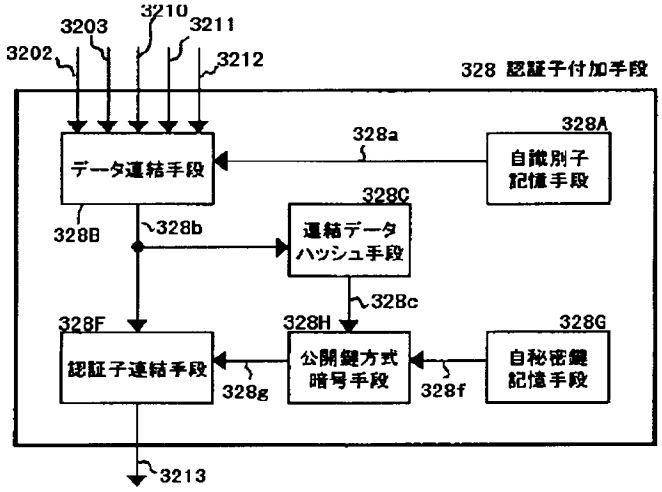
【図６】


【図6】
31
クライアント
32
認証サーバ
33
認可サーバ
ユーザID
サーバID
有効回数n
ST3101
サーバID入力
ST3102
指定サーバ用
チケットチェック
ST3103
チケットなし？
ST3104
有効回数n,
ユーザID,パスワード入力
ST3105
ユーザID,サーバID,
有効回数n送信
ST3106
チャレンジ乱数受信
ST3107
パスワード,チャレンジ乱数
の連結をハッシュ
ST3108
ハッシュ値を記憶
ST3109
ハッシュ値をさらに
n段ハッシュ
ST3110
n＋1段
ハッシュ値送信
ST3111
チケット受信
ST3112
チケットを記憶
チケット
ST3113
チケット送信
ST3114
利用回数k受信
利用回数k
ST3115
ハッシュ値を読出し
ST3116
ハッシュ値をさらに
n－k段ハッシュ
ST3117
n－k＋1段
ハッシュ値送信
n－k＋1段
ハッシュ値
ST3118
認可通知受信
認可通知
終了
チャレンジ乱数
n＋1段ハッシュ値
ST3201
ユーザID,サーバID,
有効回数n受信
ST3202
ユーザIDから
パスワードを検索
ST3203
一致あり？
ST3204
チャレンジ乱数生成送信
ST3205
パスワード,チャレンジ乱数
の連結をn＋1段ハッシュ
ST3206
n＋1段
ハッシュ値受信
ST3207
ハッシュ値
一致？
ST3211
エラー処理
ST3208
チケットID生成
ST3209
チケットID,
n＋1段ハッシュ値,
n,タイムスタンプ,
サーバID,発行者ID
の連結に認証子付加
ST3210
チケットとして送信
終了
ST3301
チケット受信
ST3302
発行者IDチェック
ST3303
有効？
ST3304
認証子検証
ST3305
誤りなし？
ST3306
宛先、有効期限チェック
ST3307
自分宛and
期限内？
ST3308
チケットリスト中を
チケットIDで検索
ST3309
一致なし？
ST3310
チケットリストに追加,
残り回数mにnを設定
ST3311
mを1減,利用回数
kにn－mを設定
ST3312
利用回数k送信
ST3313
n－k＋1段
ハッシュ値受信
ST3314
得られたn－k＋1段
ハッシュ値をさらに
k段ハッシュ
ST3315
チケットからn＋1段
ハッシュ値取出し
ST3316
ハッシュ値
一致？
ST3318
エラー処理
ST3317
認可通知送信
終了
T
F

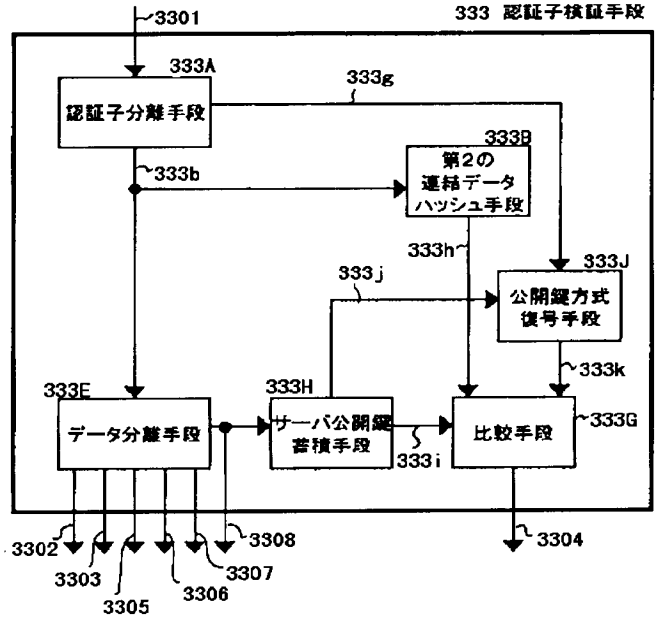
【図８】


3301
333 認証子検証手段
333A
認証子分離手段
333a
333B
第2の
連結データ
ハッシュ手段
333b
333c
333D
333C
第2の
サーバ共通鍵
記憶手段
333d
第2の
共通鍵方式
暗号手段
333e
333E
データ分離手段
発行者識別子
照合手段
333f
比較手段
333G
333F
3302
3303
3305
3306
3307
3308
3304

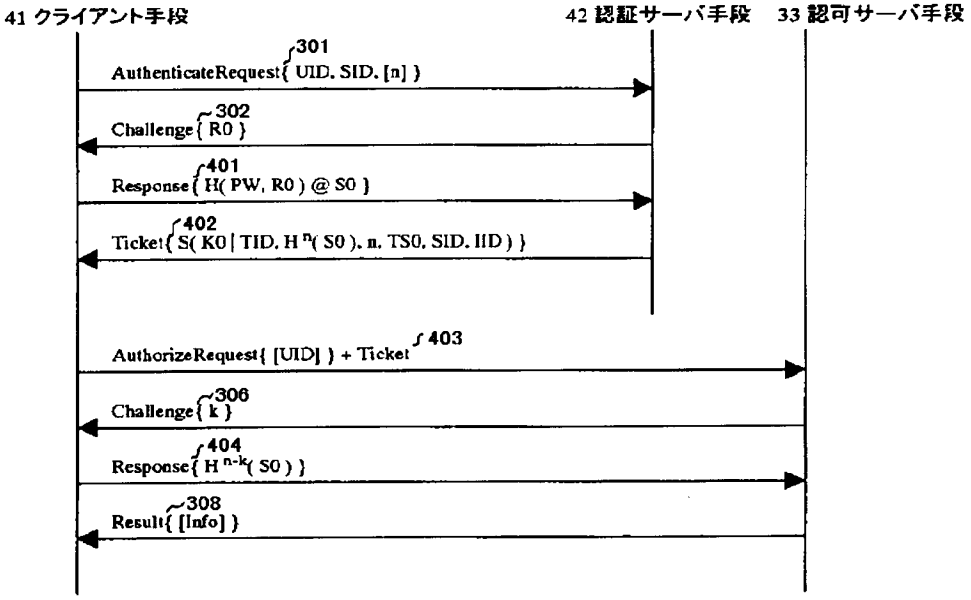
【図９】


3210
3203
3211
3202
3212
328 認証子付加手段
328A
328a
データ連結手段
自識別子
記憶手段
328C
328B
328b
連結データ
ハッシュ手段
328c
328F
328H
328G
認証子連結手段
328g
公開鍵方式
暗号手段
328f
自秘密鍵
記憶手段
3213

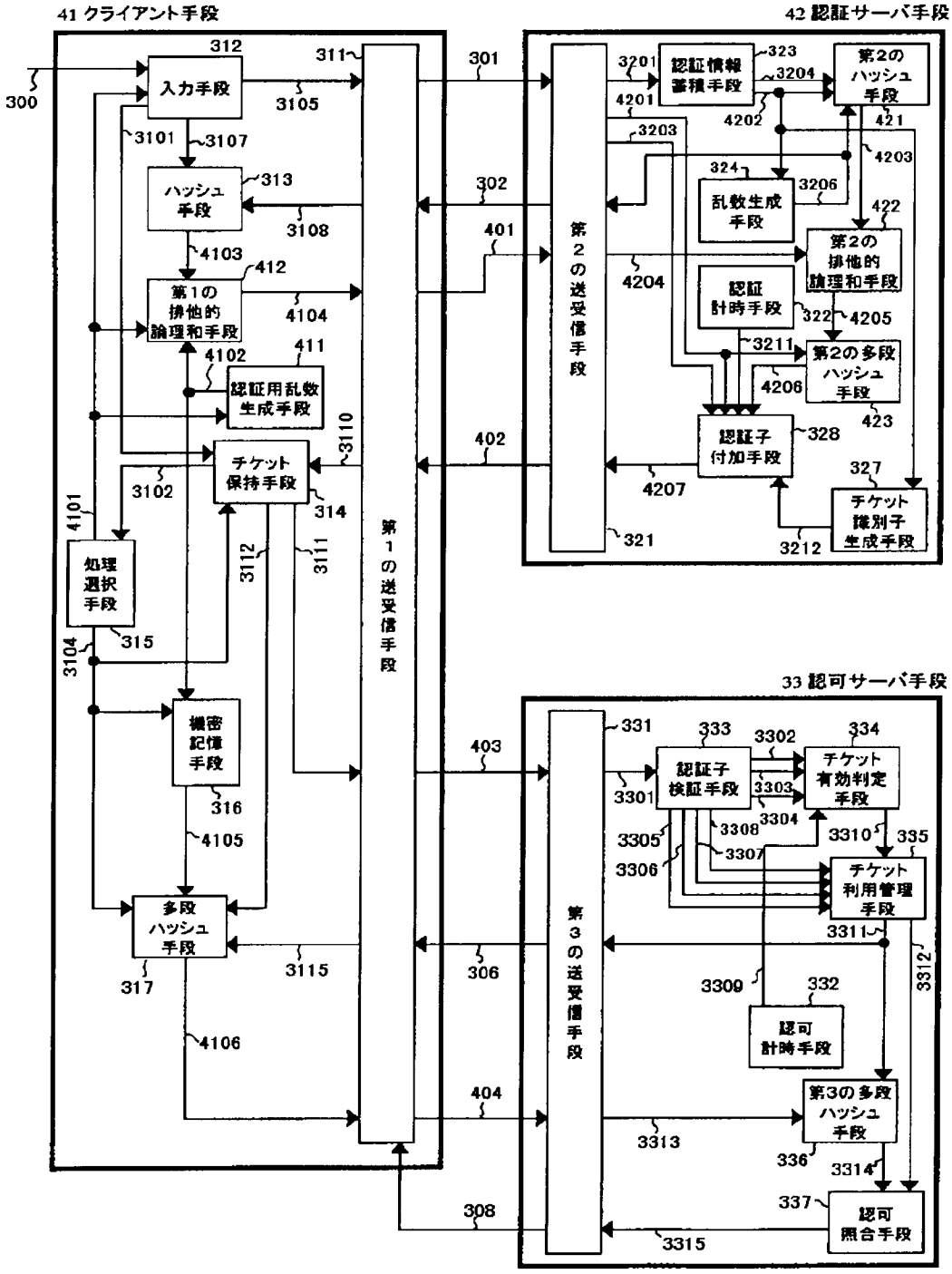
【図１０】


3301
333 認証子検証手段
333A
認証子分離手段
333g
333B
第2の
連結データ
ハッシュ手段
333b
333h
333J
333j
公開鍵方式
復号手段
333k
333E
333H
データ分離手段
サーバ公開鍵
蓄積手段
333i
比較手段
333G
3302
3303
3305
3306
3307
3308
3304

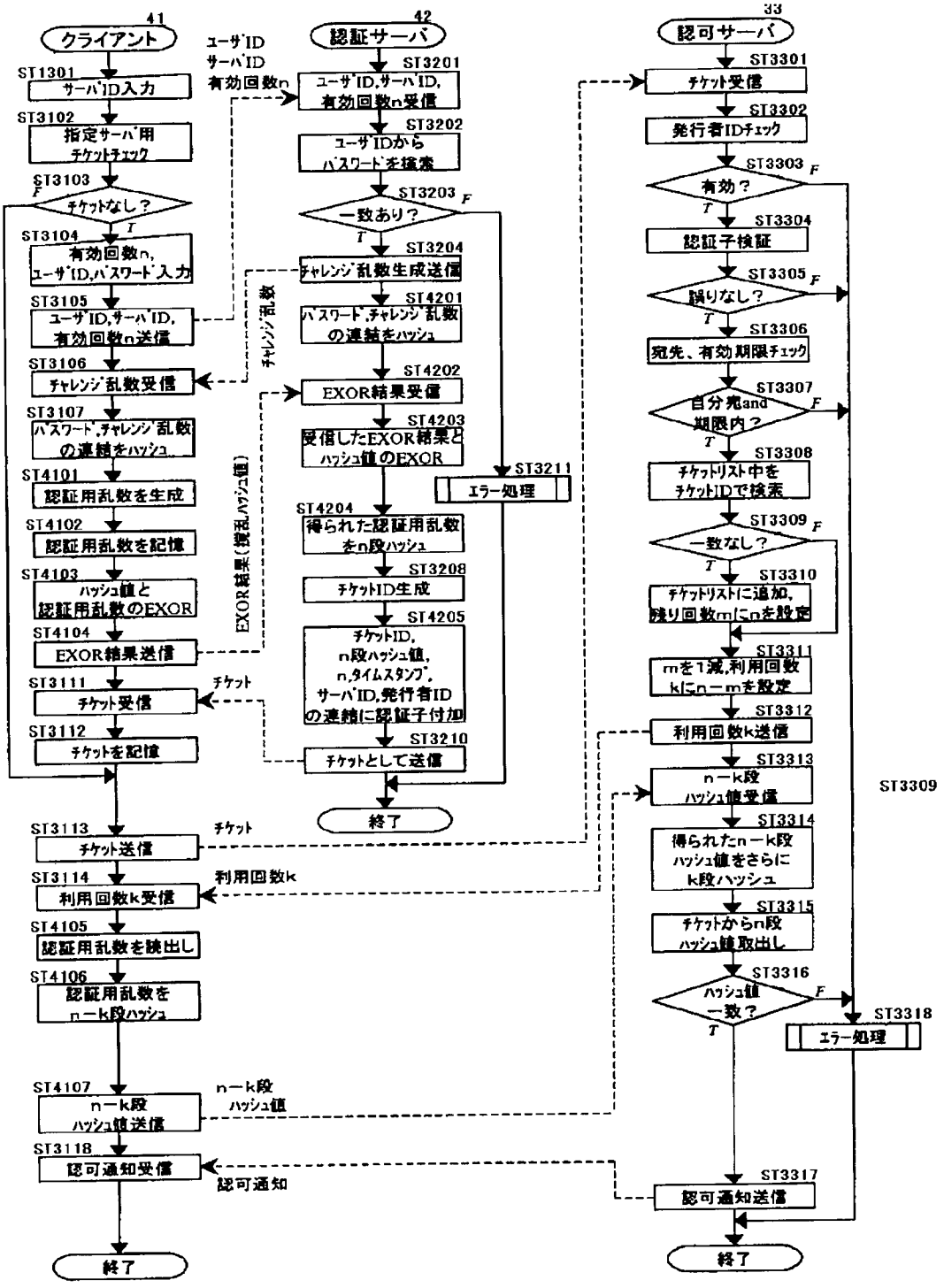
【図１１】


41 クライアント手段
42 認証サーバ手段
33 認可サーバ手段
301
AuthenticateRequest{ UID, SID, [n] }
302
Challenge{ R0 }
401
Response{ H(PW, R0) @ S0 }
402
Ticket{ S(K0 | TID, H^n(S0), n, TS0, SID, IID) }
403
AuthorizeRequest{ [UID] } + Ticket
306
Challenge{ k }
404
Response{ H^(n-k)(S0) }
308
Result{ [Info] }

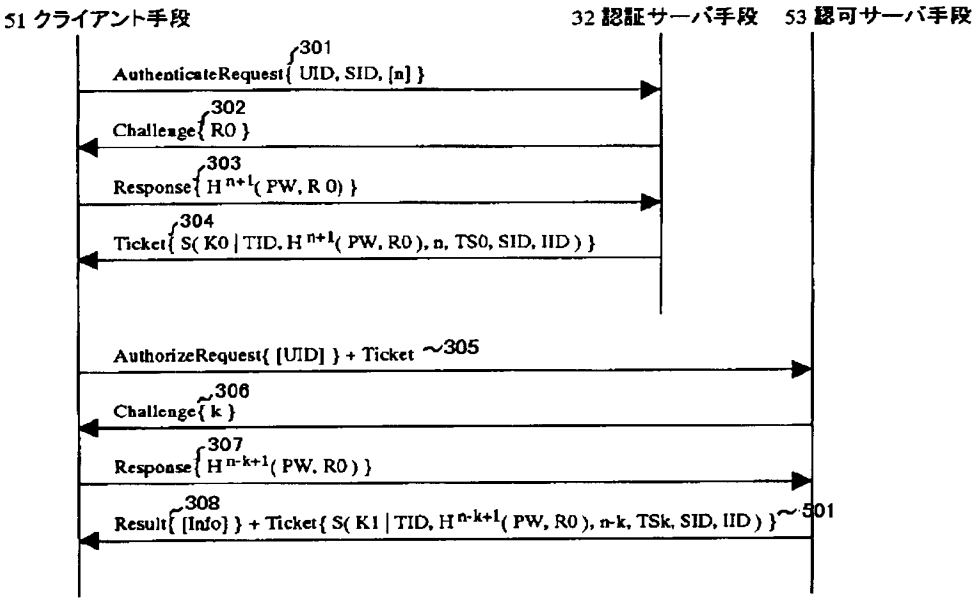
【図１２】


41 クライアント手段
42 認証サーバ手段
33 認可サーバ手段
300
入力手段
312
311
3105
301
3101
3107
ハッシュ手段
313
3108
302
401
4103
412
第1の排他的論理和手段
4104
411
4102
認証用乱数生成手段
3110
チケット保持手段
314
402
3102
4101
処理選択手段
315
3112
3111
3104
第1の送受信手段
機密記憶手段
316
4105
多段ハッシュ手段
317
3115
306
4106
404
308
第2の送受信手段
3201
認証情報蓄積手段
323
3204
第2のハッシュ手段
421
4201
4202
3203
4203
324
乱数生成手段
3206
422
第2の排他的論理和手段
4204
認証計時手段
322
4205
3211
第2の多段ハッシュ手段
4206
423
認証子付加手段
328
4207
327
チケット識別子生成手段
3212
321
403
331
333
3302
334
認証子検証手段
3301
3303
チケット有効判定手段
3304
3308
3310
335
3305
3307
3306
チケット利用管理手段
3311
3312
3309
332
認可計時手段
第3の多段ハッシュ手段
3313
336
3314
337
認可照合手段
3315
第3の送受信手段

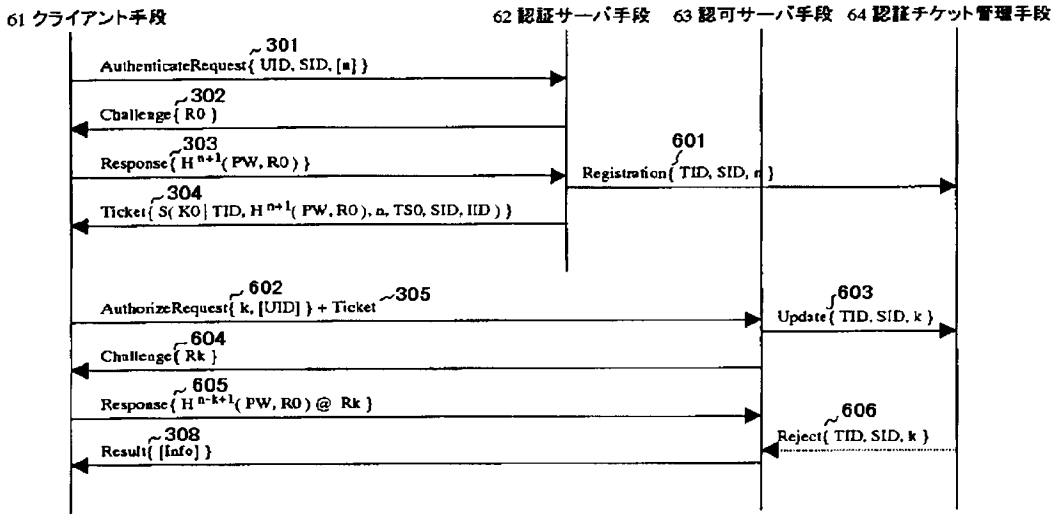
【図１３】


41
クライアント
42
認証サーバ
33
認可サーバ
ユーザID
サーバID
有効回数n
ST1301
サーバID入力
ST3102
指定サーバ用チケットチェック
ST3103
チケットなし？
F
T
ST3104
有効回数n,ユーザID,パスワード入力
ST3105
ユーザID,サーバID,有効回数n送信
ST3106
チャレンジ乱数受信
ST3107
パスワード,チャレンジ乱数の連結をハッシュ
ST4101
認証用乱数を生成
ST4102
認証用乱数を記憶
ST4103
ハッシュ値と認証用乱数のEXOR
ST4104
EXOR結果送信
ST3111
チケット受信
チケット
ST3112
チケットを記憶
ST3113
チケット送信
チケット
ST3114
利用回数k受信
利用回数k
ST4105
認証用乱数を読出し
ST4106
認証用乱数をn－k段ハッシュ
ST4107
n－k段ハッシュ値送信
n－k段ハッシュ値
ST3118
認可通知受信
認可通知
終了
ST3201
ユーザID,サーバID,有効回数n受信
ST3202
ユーザIDからパスワードを検索
ST3203
一致あり？
F
T
ST3204
チャレンジ乱数生成送信
チャレンジ乱数
ST4201
パスワード,チャレンジ乱数の連結をハッシュ
ST4202
EXOR結果受信
EXOR結果(擬乱ハッシュ値)
ST4203
受信したEXOR結果とハッシュ値のEXOR
ST3211
エラー処理
ST4204
得られた認証用乱数をn段ハッシュ
ST3208
チケットID生成
ST4205
チケットID,n段ハッシュ値,n,タイムスタンプ,サーバID,発行者IDの連結に認証子付加
ST3210
チケットとして送信
終了
ST3301
チケット受信
ST3302
発行者IDチェック
ST3303
有効？
F
T
ST3304
認証子検証
ST3305
誤りなし？
F
T
ST3306
宛先、有効期限チェック
ST3307
自分宛and期限内？
F
T
ST3308
チケットリスト中をチケットIDで検索
ST3309
一致なし？
F
T
ST3310
チケットリストに追加,残り回数mにnを設定
ST3311
mを1減,利用回数kにn－mを設定
ST3312
利用回数k送信
ST3313
n－k段ハッシュ値受信
ST3309
ST3314
得られたn－k段ハッシュ値をさらにk段ハッシュ
ST3315
チケットからn段ハッシュ値取出し
ST3316
ハッシュ値一致？
F
T
ST3318
エラー処理
ST3317
認可通知送信
終了

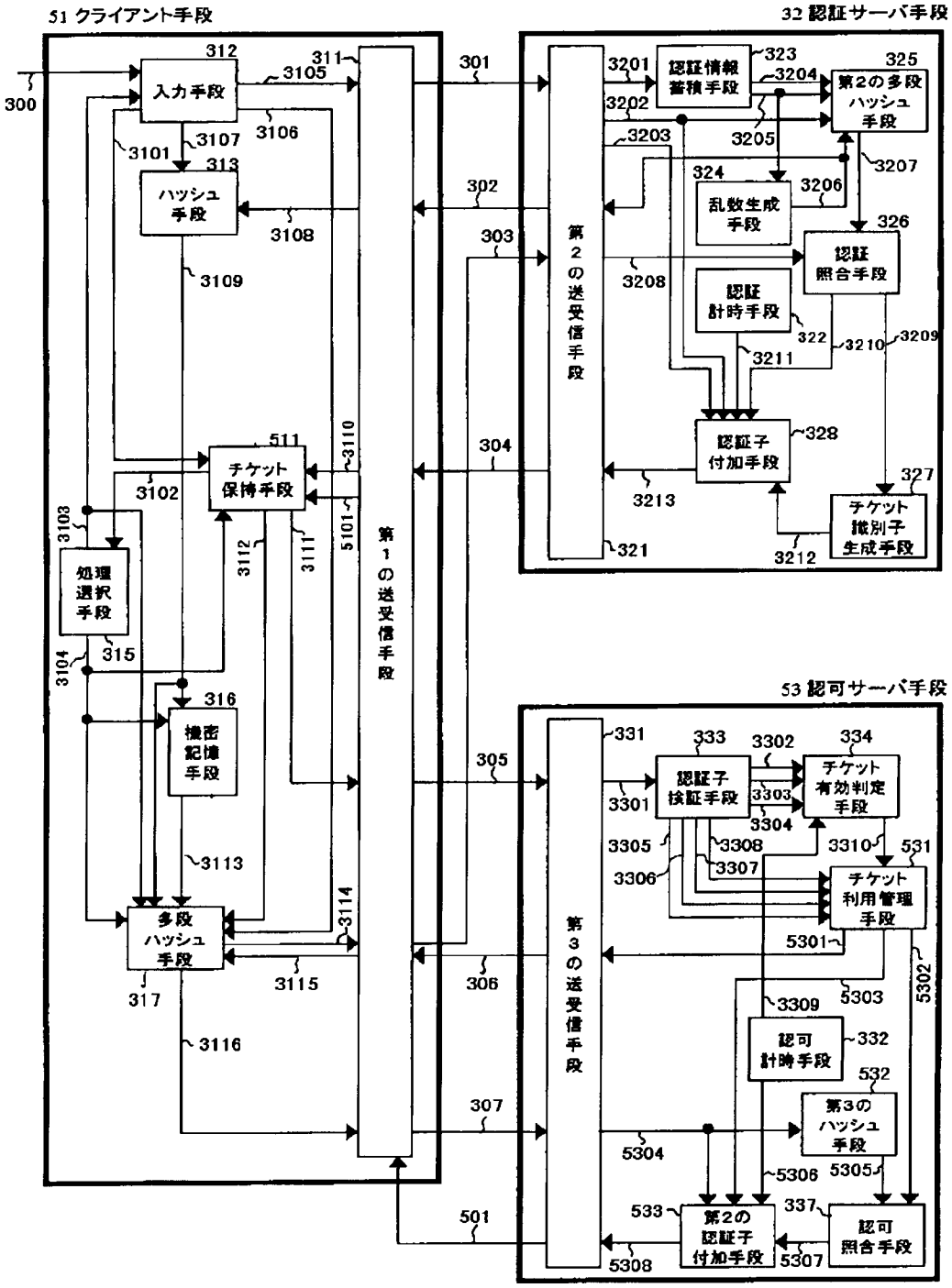
【図１４】


51 クライアント手段
32 認証サーバ手段
53 認可サーバ手段
301
AuthenticateRequest{ UID, SID, [n] }
302
Challenge{ R0 }
303
Response{ H^n+1(PW, R 0) }
304
Ticket{ S(K0 | TID, H^n+1(PW, R0), n, TS0, SID, IID) }
AuthorizeRequest{ [UID] } + Ticket
305
306
Challenge{ k }
307
Response{ H^n-k+1(PW, R0) }
308
Result{ [Info] } + Ticket{ S(K1 | TID, H^n-k+1(PW, R0), n-k, TSk, SID, IID) }
501

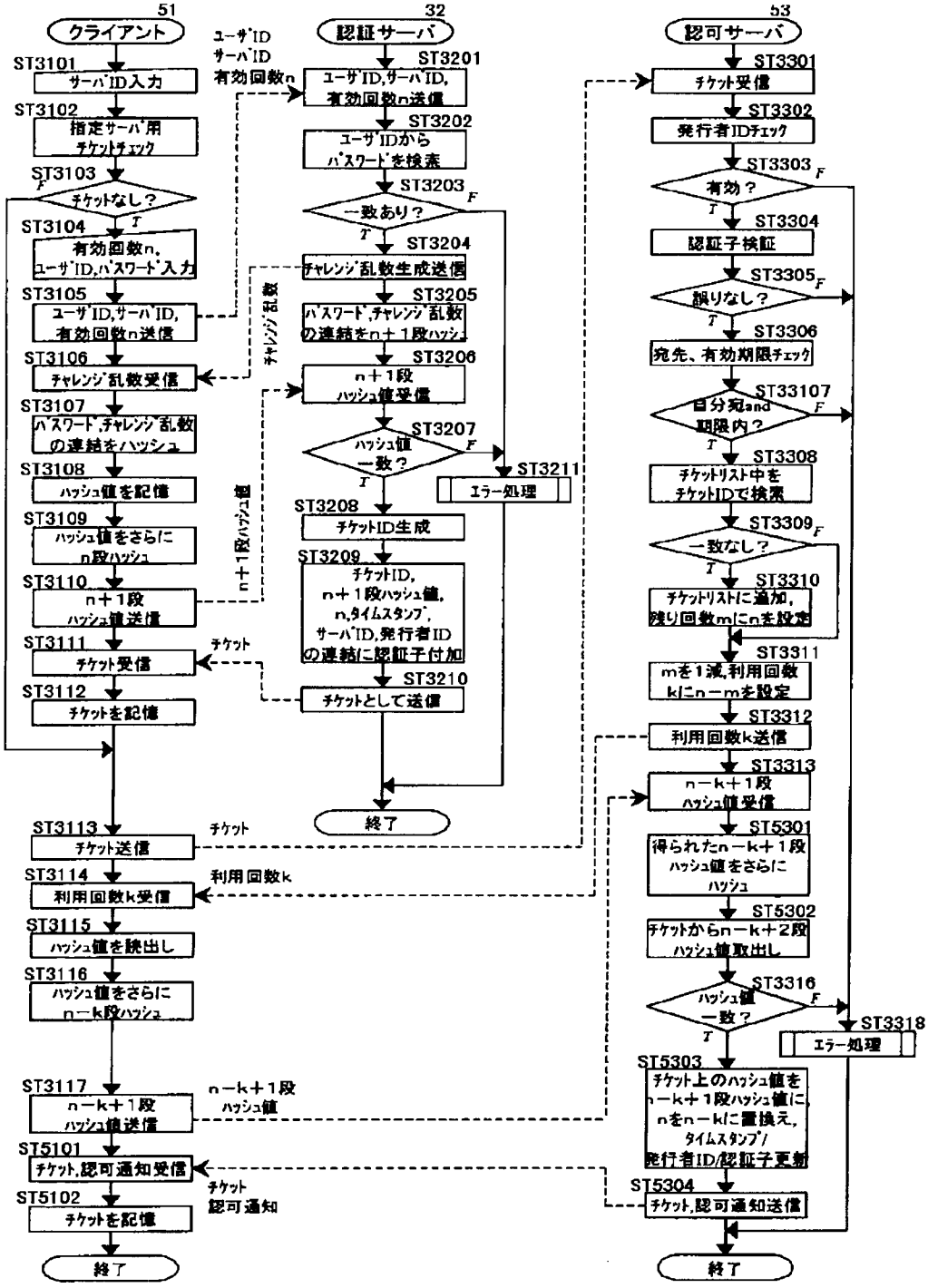
【図１７】


61 クライアント手段
62 認証サーバ手段
63 認可サーバ手段
64 認証チケット管理手段
301
AuthenticateRequest{ UID, SID, [n] }
302
Challenge{ R0 }
303
Response{ H^n+1(PW, R0) }
601
Registration{ TID, SID, n }
304
Ticket{ S(K0 | TID, H^n+1(PW, R0), n, TS0, SID, IID) }
602
AuthorizeRequest{ k, [UID] } + Ticket
305
603
Update{ TID, SID, k }
604
Challenge{ Rk }
605
Response{ H^n-k+1(PW, R0) @ Rk }
606
Reject{ TID, SID, k }
308
Result{ [Info] }

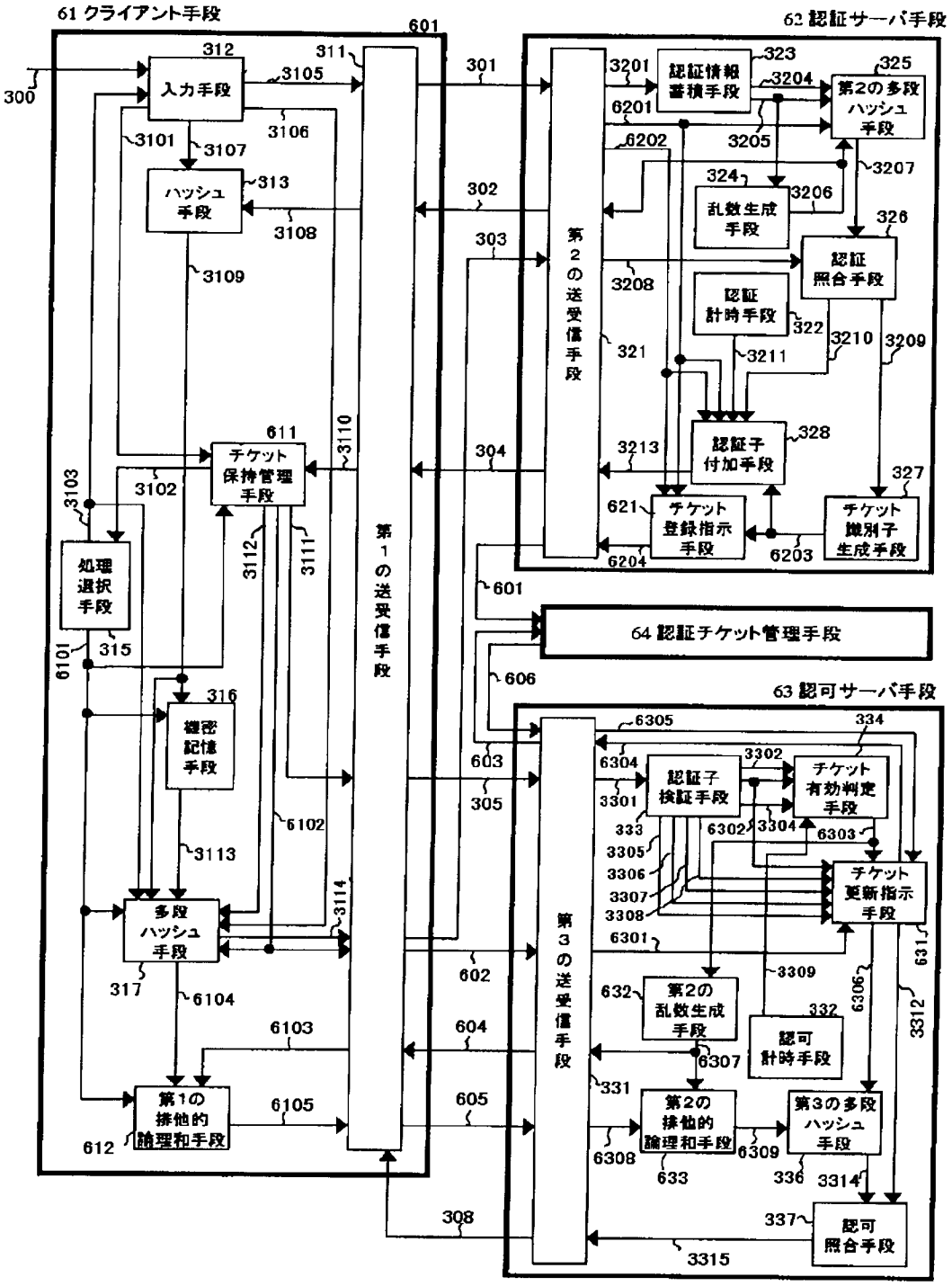
【図１５】


51 クライアント手段
32 認証サーバ手段
53 認可サーバ手段
入力手段
ハッシュ手段
チケット保持手段
処理選択手段
機密記憶手段
多段ハッシュ手段
第1の送受信手段
第2の送受信手段
第3の送受信手段
認証情報蓄積手段
第2の多段ハッシュ手段
乱数生成手段
認証照合手段
認証計時手段
認証子付加手段
チケット識別子生成手段
認証子検証手段
チケット有効判定手段
チケット利用管理手段
認可計時手段
第3のハッシュ手段
第2の認証子付加手段
認可照合手段

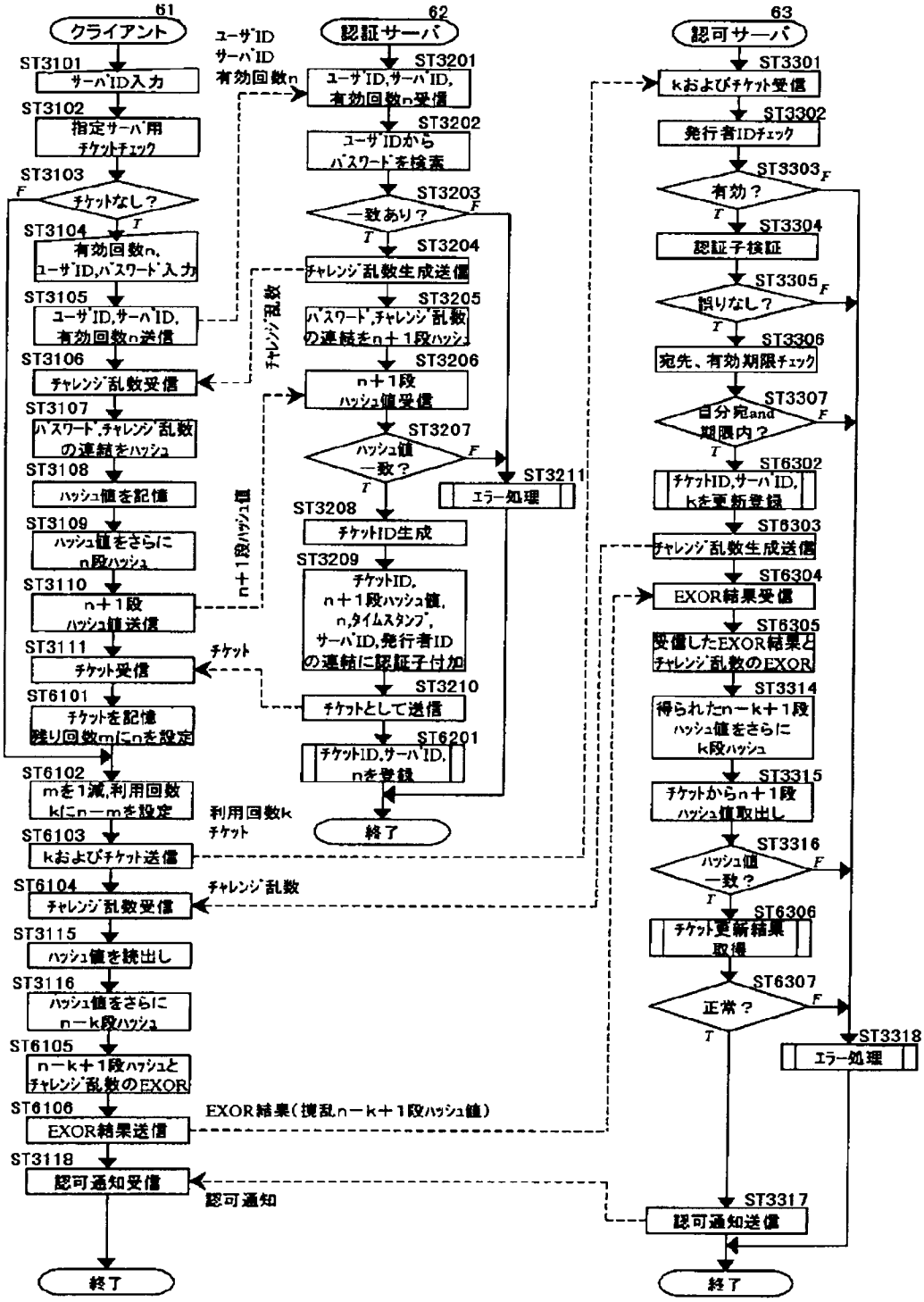
【図１６】


51
クライアント
32
認証サーバ
53
認可サーバ
ユーザID
サーバID
有効回数n
ST3101
サーバID入力
ST3102
指定サーバ用チケットチェック
ST3103
チケットなし？
ST3104
有効回数n,ユーザID,パスワード入力
ST3105
ユーザID,サーバID,有効回数n送信
ST3106
チャレンジ乱数受信
ST3107
パスワード,チャレンジ乱数の連結をハッシュ
ST3108
ハッシュ値を記憶
ST3109
ハッシュ値をさらにn段ハッシュ
ST3110
n＋1段ハッシュ値送信
ST3111
チケット受信
チケット
ST3112
チケットを記憶
ST3113
チケット送信
チケット
ST3114
利用回数k受信
利用回数k
ST3115
ハッシュ値を読出し
ST3116
ハッシュ値をさらにn－k段ハッシュ
ST3117
n－k＋1段ハッシュ値送信
n－k＋1段ハッシュ値
ST5101
チケット,認可通知受信
チケット
認可通知
ST5102
チケットを記憶
終了
ST3201
ユーザID,サーバID,有効回数n送信
ST3202
ユーザIDからパスワードを検索
ST3203
一致あり？
ST3204
チャレンジ乱数生成送信
チャレンジ乱数
ST3205
パスワード,チャレンジ乱数の連結をn＋1段ハッシュ
ST3206
n＋1段ハッシュ値受信
ST3207
ハッシュ値一致？
ST3211
エラー処理
n＋1段ハッシュ値
ST3208
チケットID生成
ST3209
チケットID,n＋1段ハッシュ値,n,タイムスタンプ,サーバID,発行者IDの連結に認証子付加
ST3210
チケットとして送信
終了
ST3301
チケット受信
ST3302
発行者IDチェック
ST3303
有効？
ST3304
認証子検証
ST3305
誤りなし？
ST3306
宛先、有効期限チェック
ST33107
自分宛and期限内？
ST3308
チケットリスト中をチケットIDで検索
ST3309
一致なし？
ST3310
チケットリストに追加,残り回数mにnを設定
ST3311
mを1減,利用回数kにn－mを設定
ST3312
利用回数k送信
ST3313
n－k＋1段ハッシュ値受信
ST5301
得られたn－k＋1段ハッシュ値をさらにハッシュ
ST5302
チケットからn－k＋2段ハッシュ値取出し
ST3316
ハッシュ値一致？
ST3318
エラー処理
ST5303
チケット上のハッシュ値をn－k＋1段ハッシュ値に,nをn－kに置換え,タイムスタンプ/発行者ID/認証子更新
ST5304
チケット,認可通知送信
終了

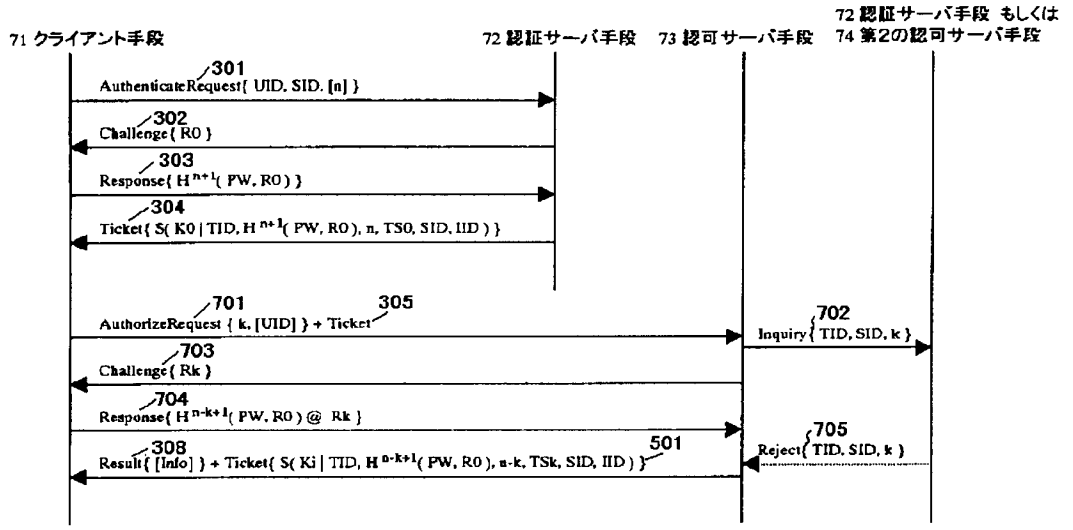
【図１８】


61 クライアント手段
62 認証サーバ手段
63 認可サーバ手段
64 認証チケット管理手段
入力手段
ハッシュ手段
チケット保持管理手段
処理選択手段
機密記憶手段
多段ハッシュ手段
第1の排他的論理和手段
第1の送受信手段
第2の送受信手段
第3の送受信手段
認証情報蓄積手段
第2の多段ハッシュ手段
乱数生成手段
認証照合手段
認証計時手段
認証子付加手段
チケット登録指示手段
チケット識別子生成手段
認証子検証手段
チケット有効判定手段
チケット更新指示手段
第2の乱数生成手段
認可計時手段
第2の排他的論理和手段
第3の多段ハッシュ手段
認可照合手段

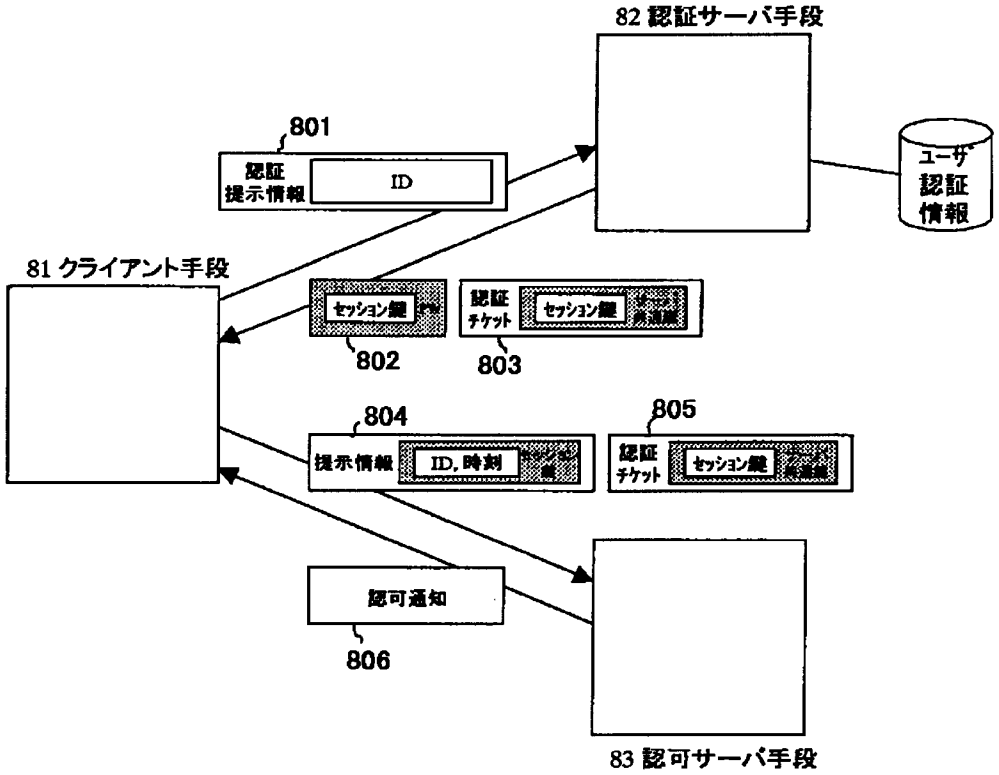
【図１９】


61
クライアント
62
認証サーバ
63
認可サーバ
ユーザID
サーバID
有効回数n
ST3101
サーバID入力
ST3102
指定サーバ用チケットチェック
ST3103
チケットなし？
F
T
ST3104
有効回数n,ユーザID,パスワード入力
ST3105
ユーザID,サーバID,有効回数n送信
ST3106
チャレンジ乱数受信
ST3107
パスワード,チャレンジ乱数の連結をハッシュ
ST3108
ハッシュ値を記憶
ST3109
ハッシュ値をさらにn段ハッシュ
ST3110
n＋1段ハッシュ値送信
ST3111
チケット受信
チケット
ST6101
チケットを記憶残り回数mにnを設定
ST6102
mを1減,利用回数kにn－mを設定
ST6103
kおよびチケット送信
利用回数k
チケット
ST6104
チャレンジ乱数受信
チャレンジ乱数
ST3115
ハッシュ値を読出し
ST3116
ハッシュ値をさらにn－k段ハッシュ
ST6105
n－k＋1段ハッシュとチャレンジ乱数のEXOR
ST6106
EXOR結果送信
EXOR結果（撹乱n－k＋1段ハッシュ値）
ST3118
認可通知受信
認可通知
終了
ST3201
ユーザID,サーバID,有効回数n受信
ST3202
ユーザIDからパスワードを検索
ST3203
一致あり？
F
T
ST3204
チャレンジ乱数生成送信
チャレンジ乱数
ST3205
パスワード,チャレンジ乱数の連結をn＋1段ハッシュ
ST3206
n＋1段ハッシュ値受信
n＋1段ハッシュ値
ST3207
ハッシュ値一致？
F
T
ST3211
エラー処理
ST3208
チケットID生成
ST3209
チケットID,n＋1段ハッシュ値,n,タイムスタンプ,サーバID,発行者IDの連結に認証子付加
ST3210
チケットとして送信
ST6201
チケットID,サーバID,nを登録
終了
ST3301
kおよびチケット受信
ST3302
発行者IDチェック
ST3303
有効？
F
T
ST3304
認証子検証
ST3305
誤りなし？
F
T
ST3306
宛先、有効期限チェック
ST3307
自分宛and期限内？
F
T
ST6302
チケットID,サーバID,kを更新登録
ST6303
チャレンジ乱数生成送信
ST6304
EXOR結果受信
ST6305
受信したEXOR結果とチャレンジ乱数のEXOR
ST3314
得られたn－k＋1段ハッシュ値をさらにk段ハッシュ
ST3315
チケットからn＋1段ハッシュ値取出し
ST3316
ハッシュ値一致？
F
T
ST6306
チケット更新結果取得
ST6307
正常？
F
T
ST3318
エラー処理
ST3317
認可通知送信
終了

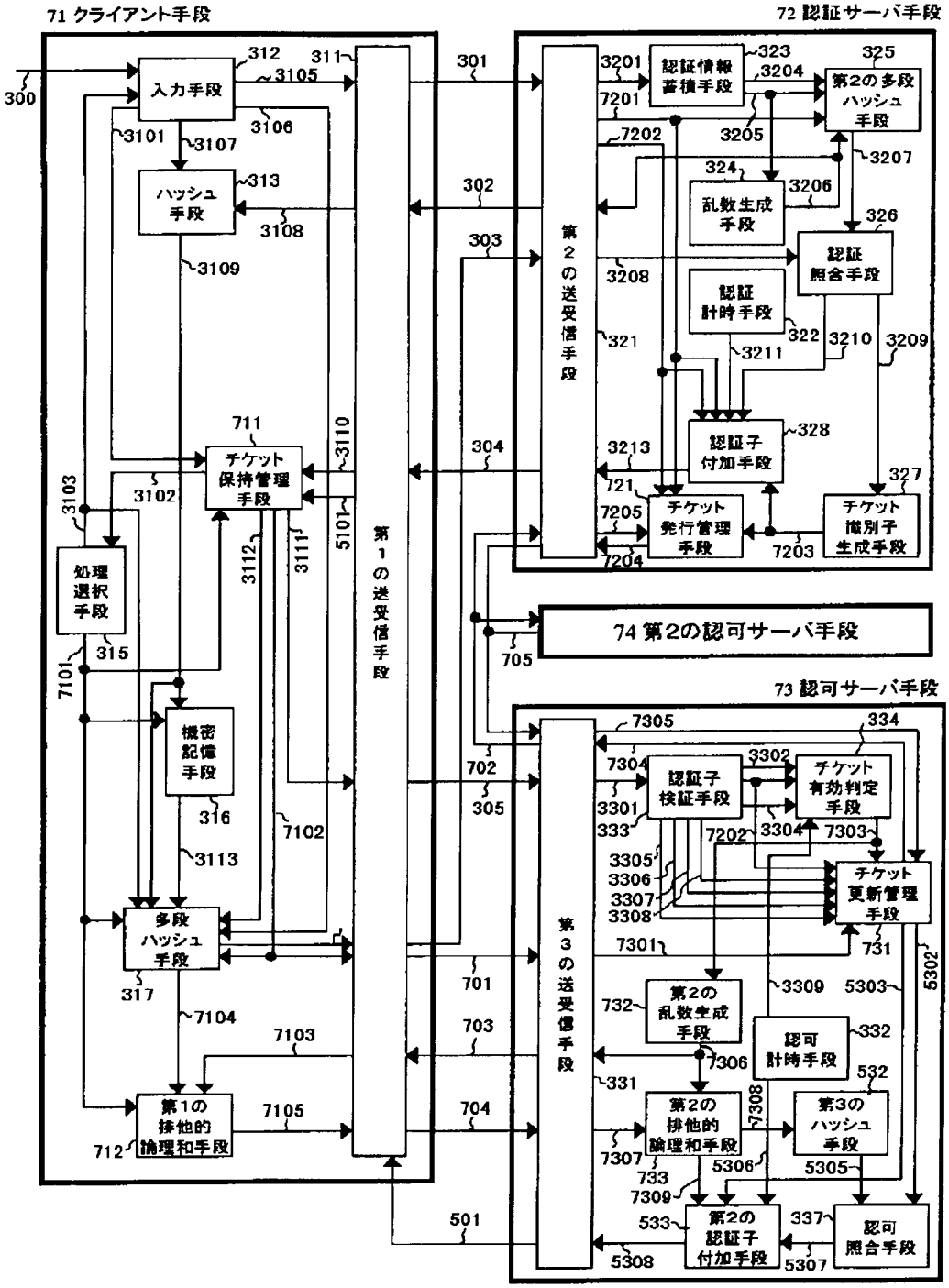
【図２０】


71 クライアント手段
72 認証サーバ手段
73 認可サーバ手段
72 認証サーバ手段 もしくは
74 第2の認可サーバ手段
301
AuthenticateRequest{ UID, SID, [n] }
302
Challenge{ R0 }
303
Response{ H^n+1(PW, R0) }
304
Ticket{ S(K0 | TID, H^n+1(PW, R0), n, TS0, SID, IID) }
701
305
AuthorizeRequest { k, [UID] } + Ticket
702
Inquiry{ TID, SID, k }
703
Challenge{ Rk }
704
Response{ H^n-k+1(PW, R0) @ Rk }
705
Reject{ TID, SID, k }
308
501
Result{ [Info] } + Ticket{ S(Ki | TID, H^n-k+1(PW, R0), n-k, TSk, SID, IID) }

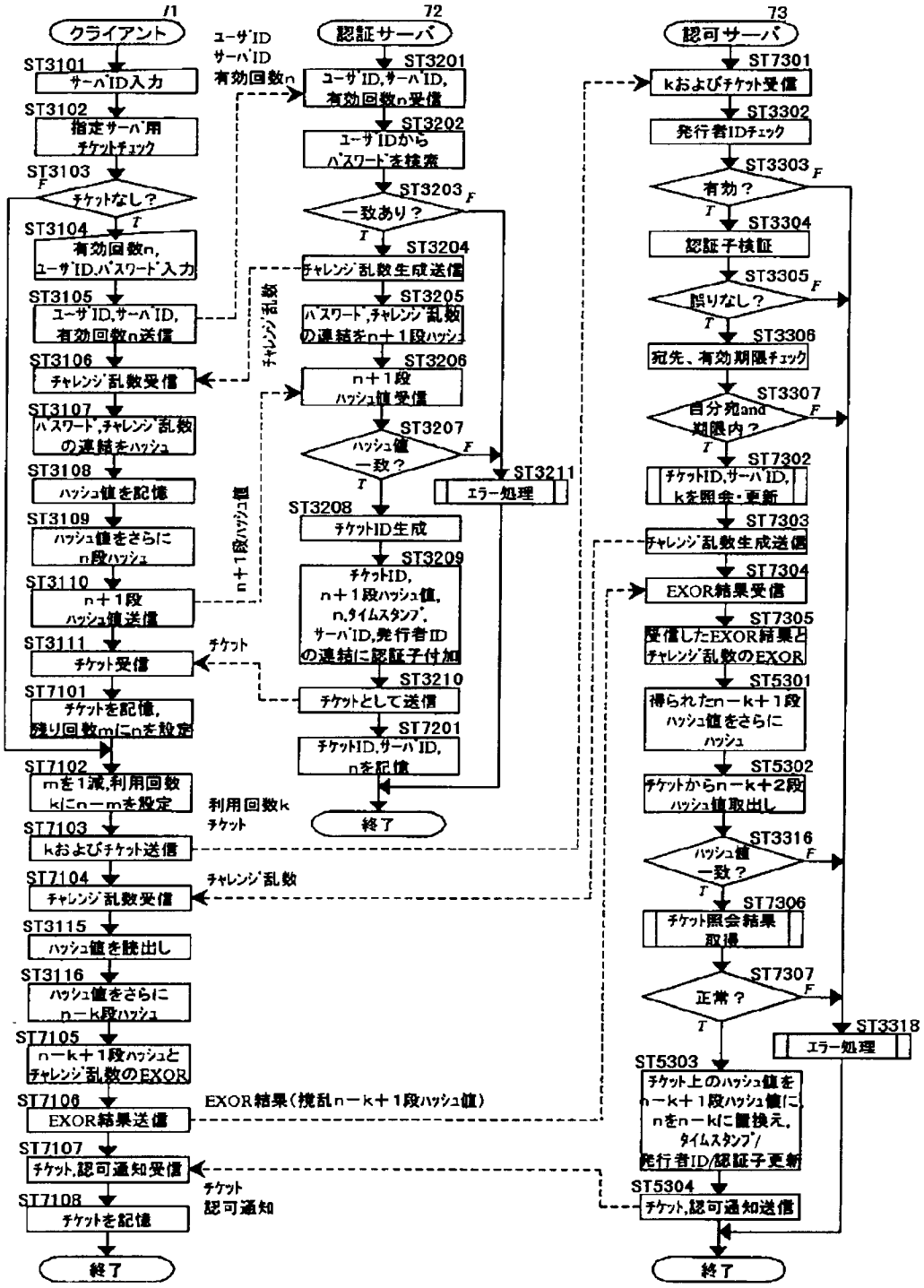
【図２３】


82 認証サーバ手段
801
認証
提示情報
ID
ユーザ
認証
情報
81 クライアント手段
セッション鍵
認証
チケット
セッション鍵
802
803
804
805
提示情報
ID, 時刻
認証
チケット
セッション鍵
認可通知
806
83 認可サーバ手段

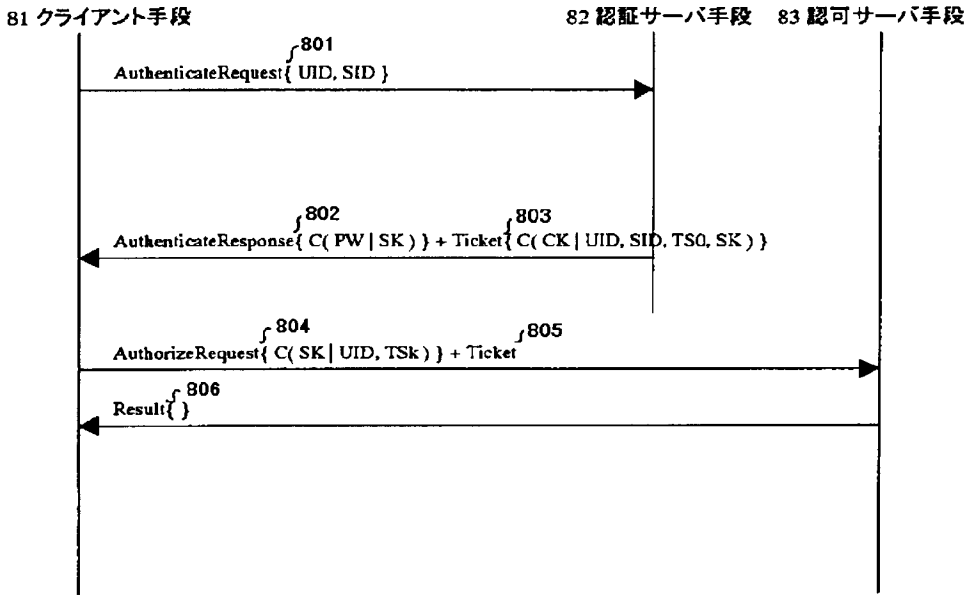
【図２１】


71 クライアント手段
72 認証サーバ手段
73 認可サーバ手段
74 第2の認可サーバ手段
入力手段
ハッシュ手段
チケット保持管理手段
処理選択手段
機密記憶手段
多段ハッシュ手段
第1の排他的論理和手段
第1の送受信手段
第2の送受信手段
第3の送受信手段
認証情報蓄積手段
第2の多段ハッシュ手段
乱数生成手段
認証照合手段
認証計時手段
認証子付加手段
チケット発行管理手段
チケット識別子生成手段
認証子検証手段
チケット有効判定手段
チケット更新管理手段
第2の乱数生成手段
認可計時手段
第2の排他的論理和手段
第3のハッシュ手段
第2の認証子付加手段
認可照合手段

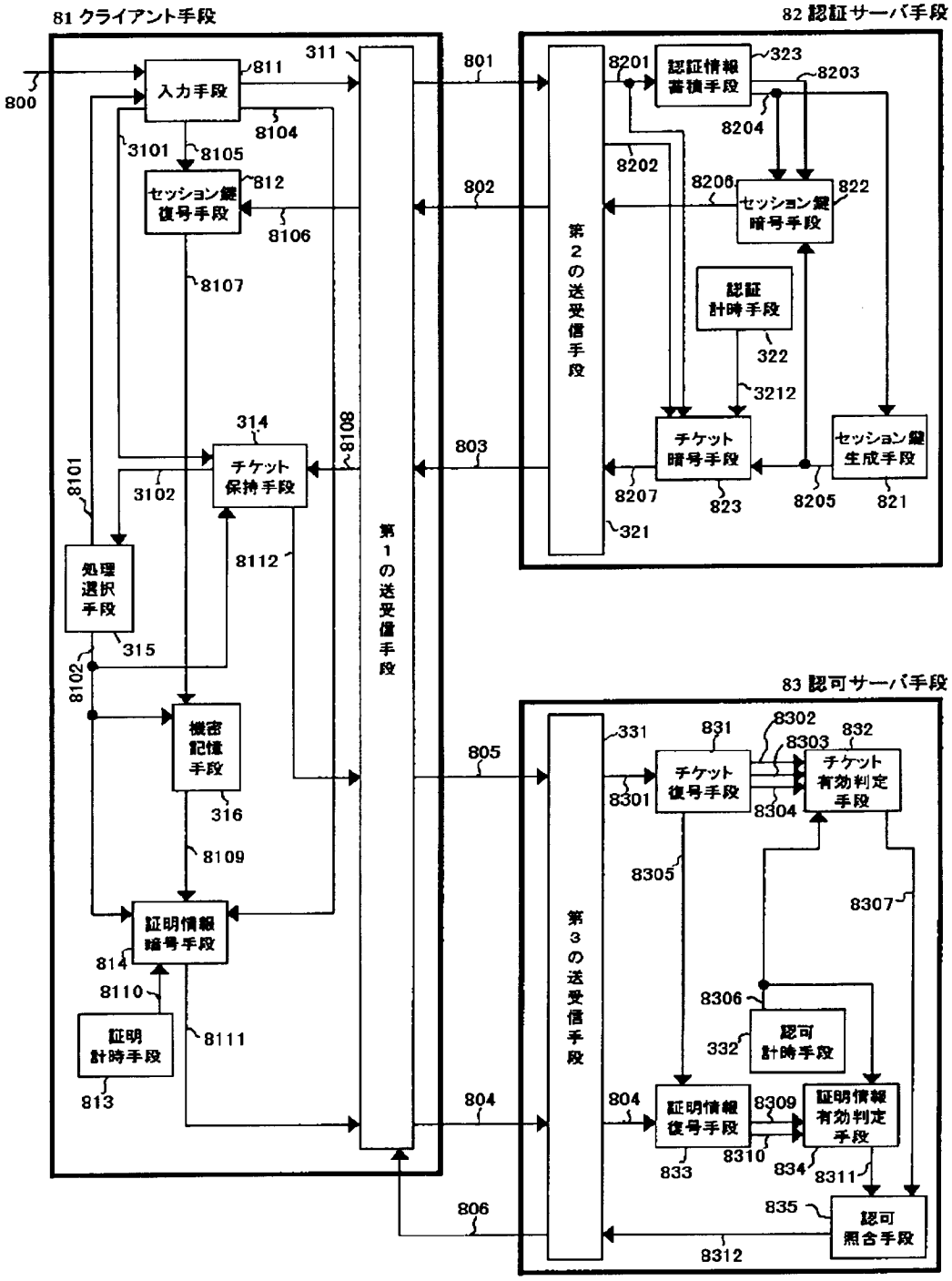
【図２２】


71
クライアント
ST3101
サーバID入力
ST3102
指定サーバ用チケットチェック
ST3103
チケットなし？
F
T
ST3104
有効回数n，ユーザID，パスワード入力
ST3105
ユーザID，サーバID，有効回数n送信
ST3106
チャレンジ乱数受信
ST3107
パスワード，チャレンジ乱数の連結をハッシュ
ST3108
ハッシュ値を記憶
ST3109
ハッシュ値をさらにn段ハッシュ
ST3110
n＋1段ハッシュ値送信
ST3111
チケット受信
ST7101
チケットを記憶，残り回数mにnを設定
ST7102
mを1減，利用回数kにn－mを設定
ST7103
kおよびチケット送信
ST7104
チャレンジ乱数受信
ST3115
ハッシュ値を読出し
ST3116
ハッシュ値をさらにn－k段ハッシュ
ST7105
n－k＋1段ハッシュとチャレンジ乱数のEXOR
ST7106
EXOR結果送信
ST7107
チケット，認可通知受信
ST7108
チケットを記憶
終了
ユーザID
サーバID
有効回数n
チャレンジ乱数
n＋1段ハッシュ値
チケット
利用回数k
チケット
チャレンジ乱数
EXOR結果（撹乱n－k＋1段ハッシュ値）
チケット
認可通知
72
認証サーバ
ST3201
ユーザID，サーバID，有効回数n受信
ST3202
ユーザIDからパスワードを検索
ST3203
一致あり？
F
T
ST3204
チャレンジ乱数生成送信
ST3205
パスワード，チャレンジ乱数の連結をn＋1段ハッシュ
ST3206
n＋1段ハッシュ値受信
ST3207
ハッシュ値一致？
F
T
ST3211
エラー処理
ST3208
チケットID生成
ST3209
チケットID，n＋1段ハッシュ値，n，タイムスタンプ，サーバID，発行者IDの連結に認証子付加
ST3210
チケットとして送信
ST7201
チケットID，サーバID，nを記憶
終了
73
認可サーバ
ST7301
kおよびチケット受信
ST3302
発行者IDチェック
ST3303
有効？
F
T
ST3304
認証子検証
ST3305
誤りなし？
F
T
ST3306
宛先，有効期限チェック
ST3307
自分宛and期限内？
F
T
ST7302
チケットID，サーバID，kを照会・更新
ST7303
チャレンジ乱数生成送信
ST7304
EXOR結果受信
ST7305
受信したEXOR結果とチャレンジ乱数のEXOR
ST5301
得られたn－k＋1段ハッシュ値をさらにハッシュ
ST5302
チケットからn－k＋2段ハッシュ値取出し
ST3316
ハッシュ値一致？
F
T
ST7306
チケット照会結果取得
ST7307
正常？
F
T
ST3318
エラー処理
ST5303
チケット上のハッシュ値をn－k＋1段ハッシュ値に，nをn－kに置換え，タイムスタンプ/発行者ID/認証子更新
ST5304
チケット，認可通知送信
終了

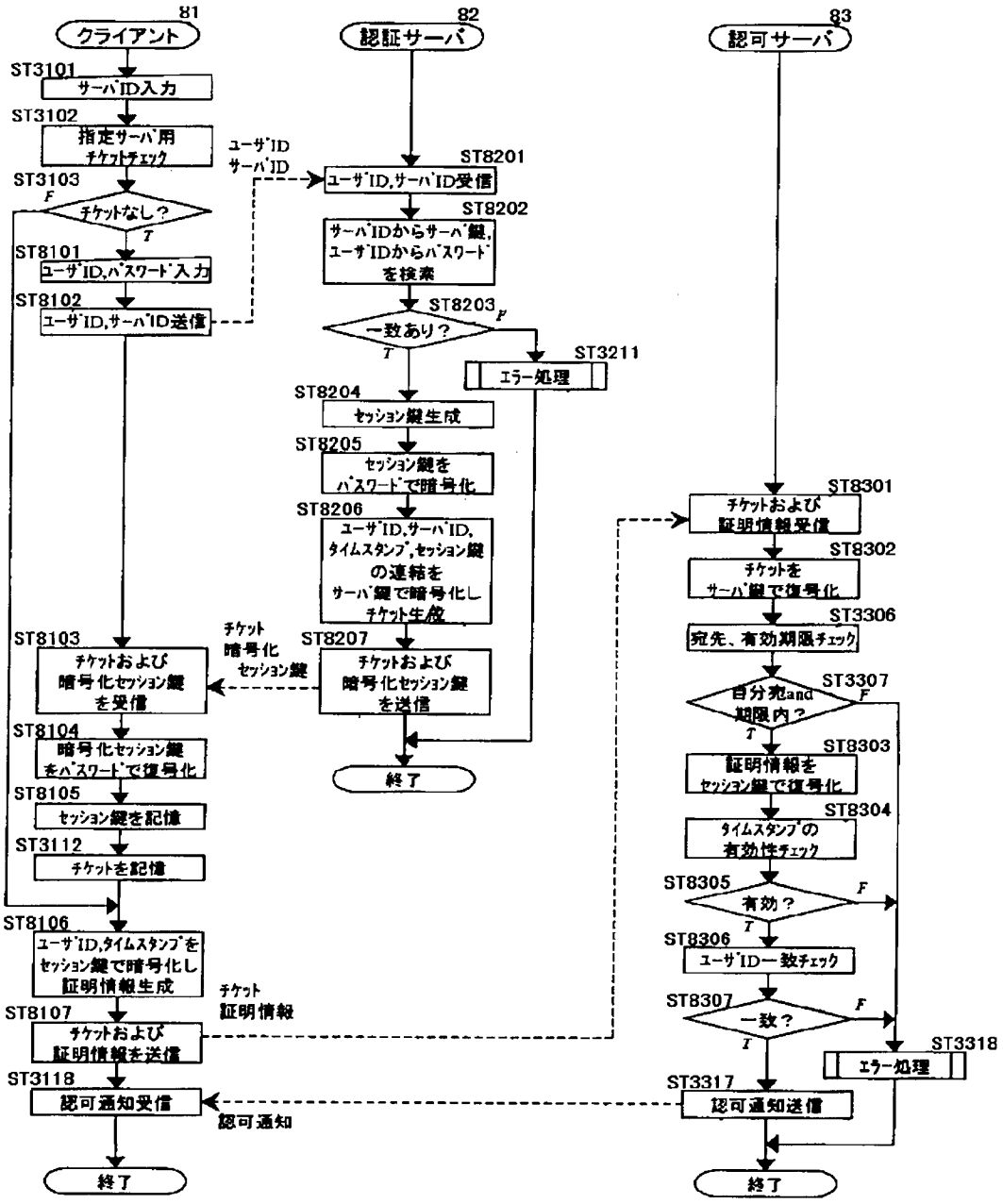
【図２４】


81 クライアント手段
82 認証サーバ手段
83 認可サーバ手段
801
AuthenticateRequest{ UID, SID }
802
AuthenticateResponse{ C(PW | SK) } + Ticket
803
{ C(CK | UID, SID, TS0, SK) }
804
AuthorizeRequest{ C(SK | UID, TSk) } + Ticket
805
806
Result{ }

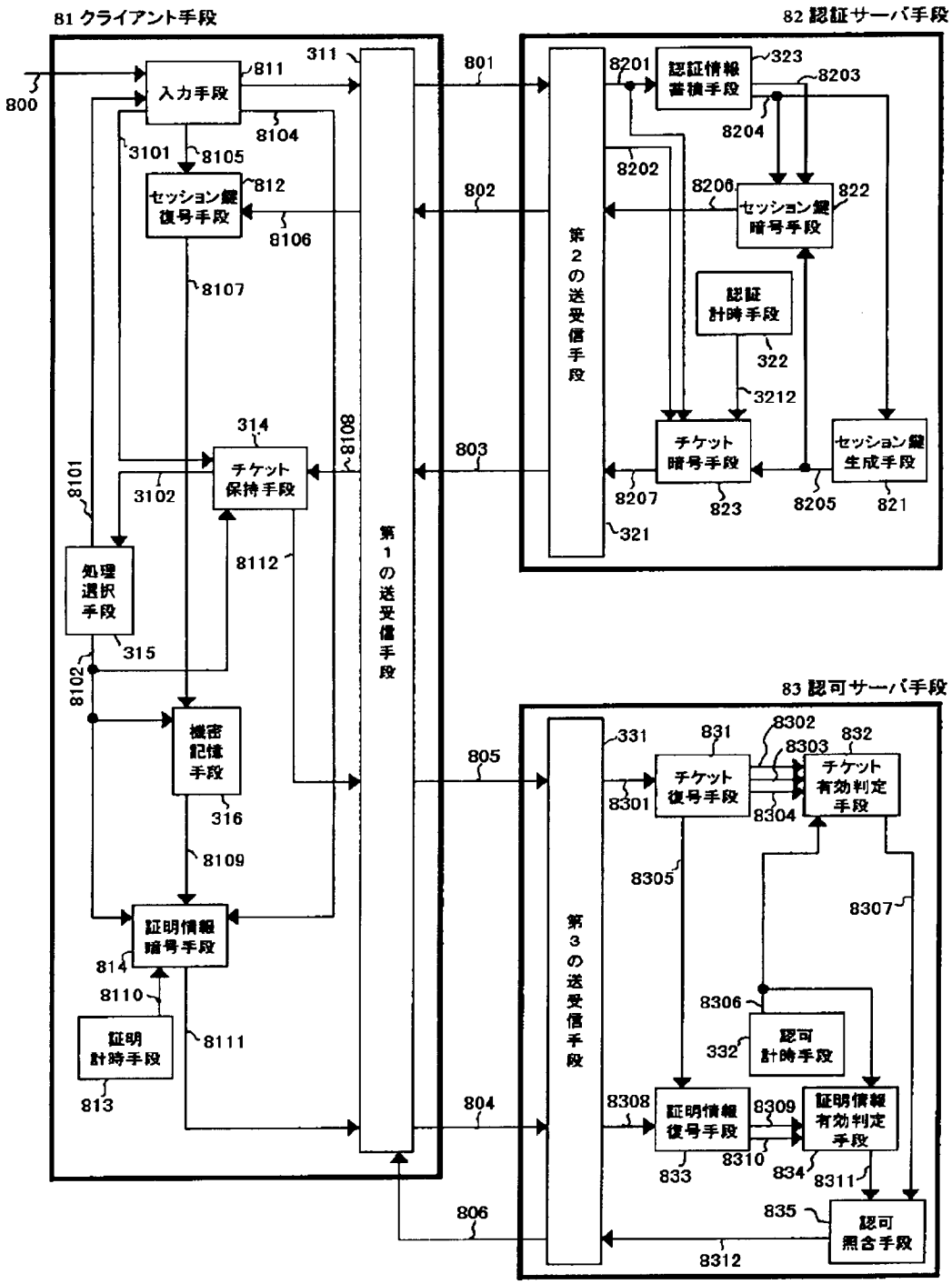
【図２５】


81 クライアント手段
82 認証サーバ手段
83 認可サーバ手段
800
入力手段
811
311
801
8201
認証情報蓄積手段
323
8203
8204
3101
8105
8104
セッション鍵復号手段
812
8106
802
8202
8206
セッション鍵暗号手段
822
8107
認証計時手段
322
3212
第2の送受信手段
314
8108
チケット保持手段
803
チケット暗号手段
セッション鍵生成手段
8101
3102
8207
823
8205
821
321
処理選択手段
8112
315
8102
機密記憶手段
316
805
331
831
8302
832
8303
チケット復号手段
チケット有効判定手段
8301
8304
8109
8305
8307
第3の送受信手段
証明情報暗号手段
814
8110
8306
認可計時手段
332
証明計時手段
8111
813
804
804
証明情報復号手段
8309
証明情報有効判定手段
8310
833
834
8311
806
835
認可照合手段
8312
第1の送受信手段

【図２６】



【手続補正書】
【提出日】平成１１年２月２日（１９９９．２．２）
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】図２５
【補正方法】変更
【補正内容】
【図２５】


81 クライアント手段
82 認証サーバ手段
83 認可サーバ手段
800
入力手段
811
311
801
認証情報蓄積手段
8201
323
8203
8204
3101
8105
8104
セッション鍵復号手段
812
802
8106
8202
8206
セッション鍵暗号手段
822
第2の送受信手段
8107
認証計時手段
322
3212
314
8108
チケット保持手段
803
チケット暗号手段
セッション鍵生成手段
8101
3102
8207
823
8205
821
321
処理選択手段
8112
315
8102
機密記憶手段
805
316
8109
第1の送受信手段
331
831
8302
832
8303
チケット復号手段
チケット有効判定手段
8301
8304
8305
8307
証明情報暗号手段
814
8110
8306
認可計時手段
332
証明計時手段
8111
813
8308
証明情報復号手段
8309
証明情報有効判定手段
804
第3の送受信手段
8310
833
834
8311
806
835
認可照合手段
8312

フロントページの続き

Ｆターム(参考) 5B017 AA01 AA07 BA05 BA07 BB03
BB07 BB10 CA16
5B058 KA33 KA40
5B085 AE01 AE06 AE09 AE13 AE23
BC01 BG07
5B089 GA11 GA21 GB03 KA17 KB13
KC58
5J104 AA07 KA01 KA04 PA07